DNSSEC

Solving A Decades-Old Vulnerability

Carlos Meza
carlos@digitalr00ts.com
@digitalr00ts

Whoami

Carlos Meza

- Sysadmin
- Likes: Open Source, Devops, InfoSec
- Learn of DNSSEC at InteropNet

carlos@digitalr00ts.com

@digitalr00ts

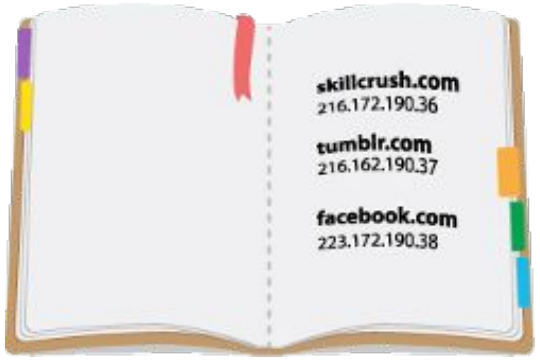
DNS

is the phonebook
of the Internet

and

DNSSEC

is unspoofable
caller ID



DNS
pairs user friendly labels to Internet network addresses

DNSSEC
ensures accuracy of that information

BENEFITS OF DNSSEC

- Protects users
- Strengthens trust in the Internet
- New possibilities

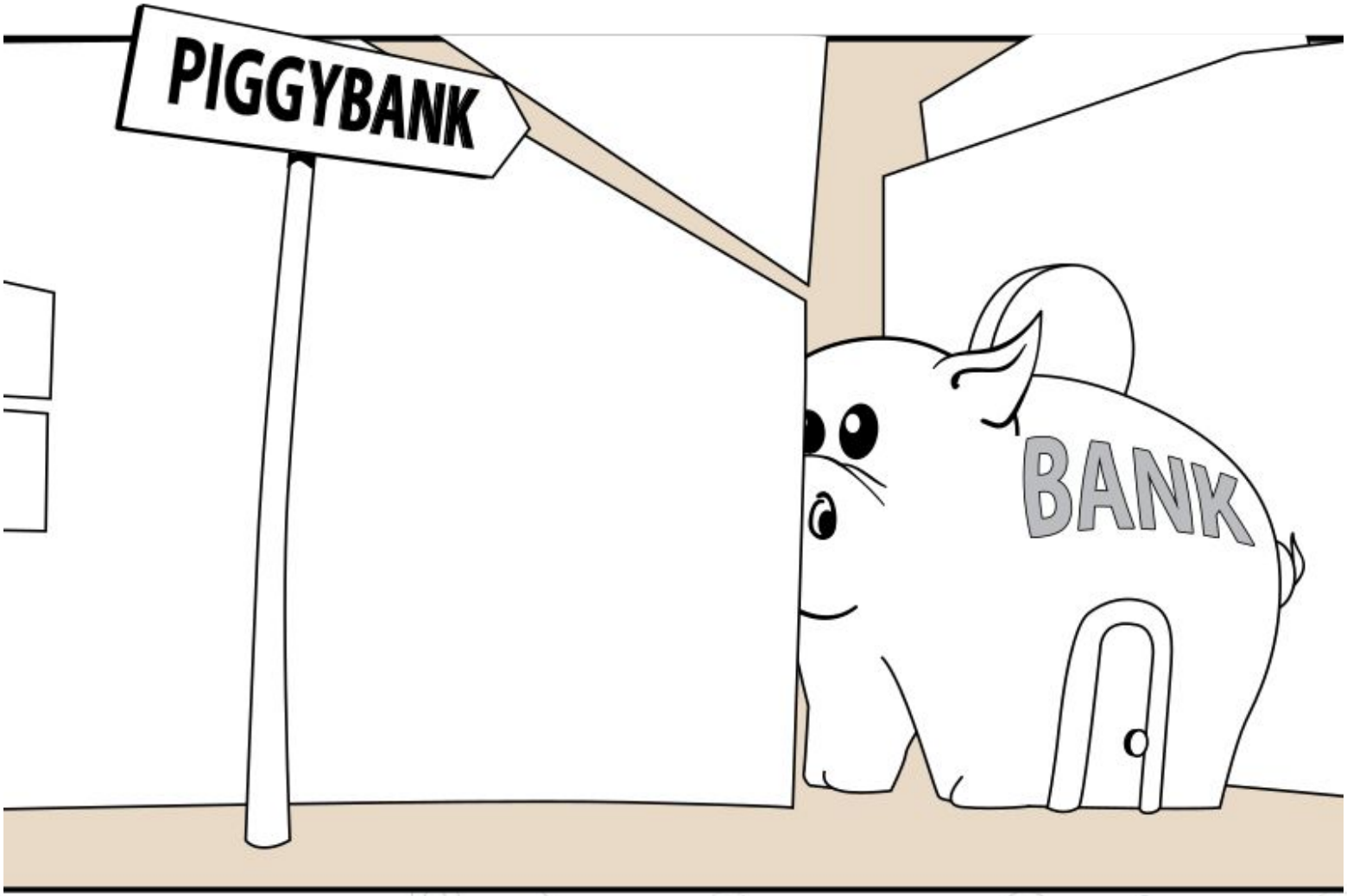
Concluding for Businesses

- Mitigate risk of cyber crime
- Protect business and brand image
- Build reputation as prioritizing security and protecting customers

The Problem with DNS

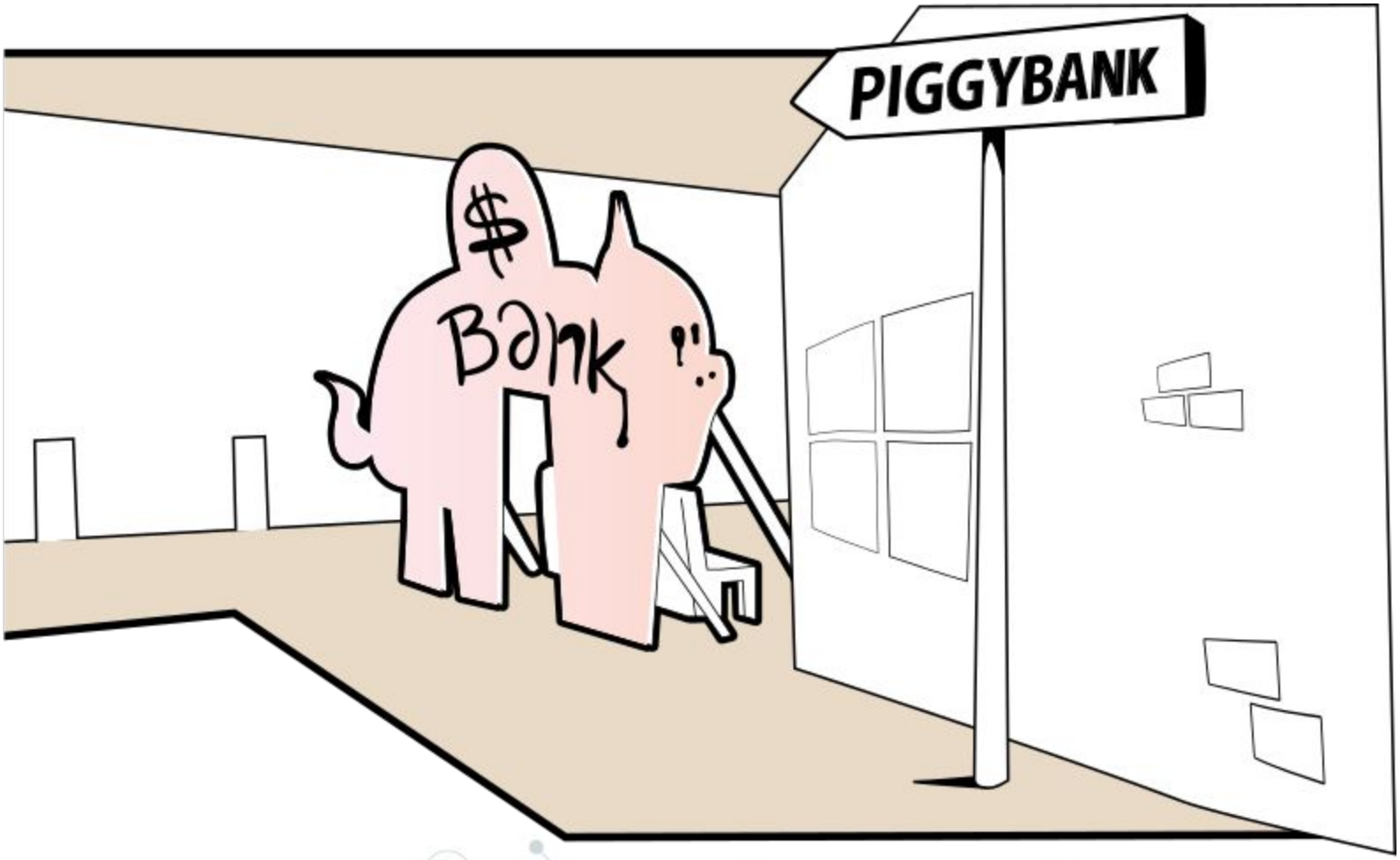
What's the big deal?

DNS data can be disrupted and fake data inserted



DNS data can be disrupted and fake data inserted

DNS data can be disrupted and fake data inserted



RISKS

An attackers can:

- Steal passwords/credentials, credit card info, identity, etc (a.k.a phishing)
- Bypass anti-spam protection
- Disseminate misinformation
- Redirect (wiretap) on phone calls (VoIP)
- Spread malicious software

DNSSEC

- Ensures credibility of DNS information.
- Protects against data spoofing and corruption.
- Adds security, while maintaining backwards compatibility.

How does all this work?

DNS Basics

TERMINOLOGY

IP Address is a unique identifying string of numbers given to every device on the Internet.

IPv4: 93.184.216.34

IPv6: 2606:2800:220:1:248:1893:25c8:1946

TERMINOLOGY

Domain Name identifies an entity on the Internet by a human readable alphanumeric name.

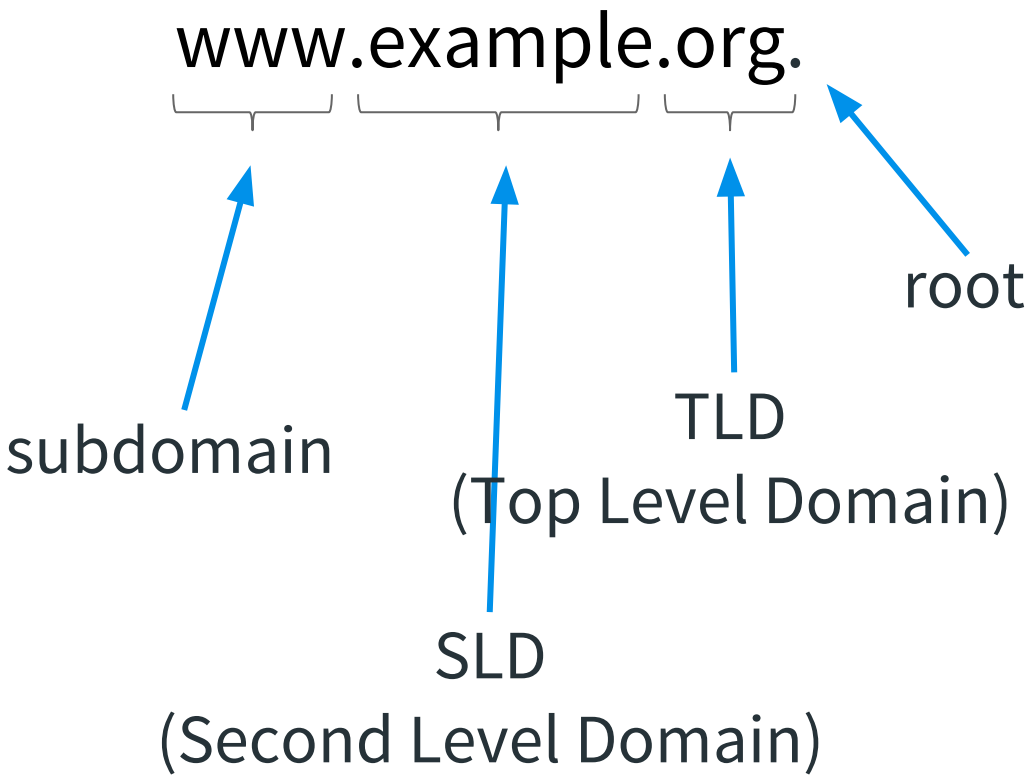
FQDN: www.example.org

Terminology

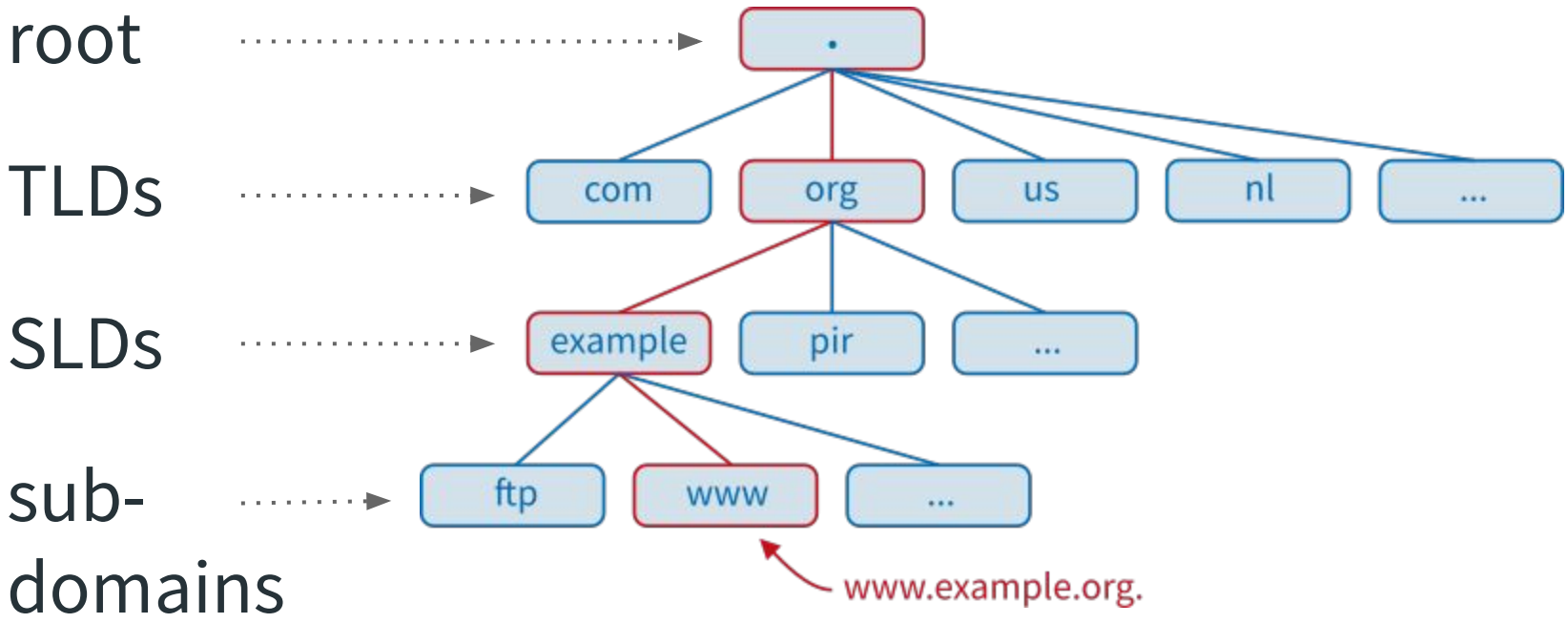
DNS (Domain Name System) is the mediator between the IP addresses and domain names.

FQDN:	www.example.org
	to
IPv4:	93.184.216.34
IPv6:	2606:2800:220:1:248:1893:25c8:1946

Anatomy of a Domain Name



DNS HIERARCHY



Terminology

Zones are delegated subsets of the hierarchical DNS structure

Resource Records (RR) are the data in zones, such the mappings between domain names and IP addresses.

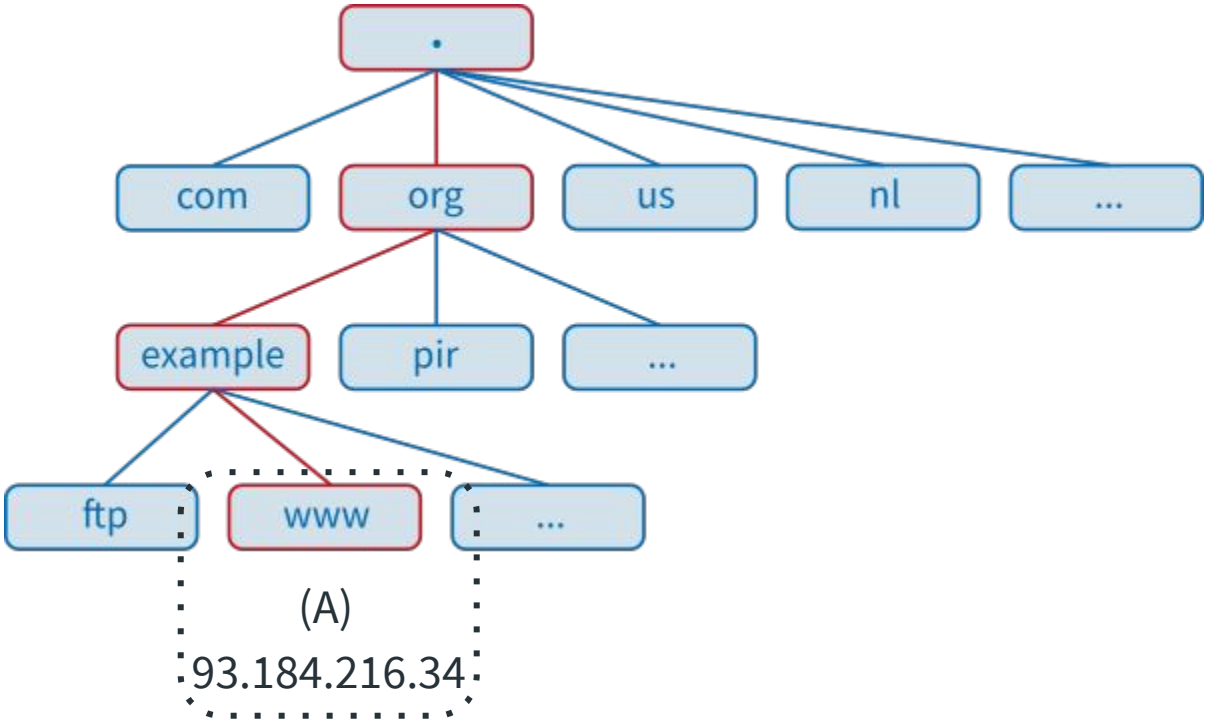
RESOURCE RECORDS (RR) EXAMPLES

A/AAAA - A Host Address IPv4/IPv6

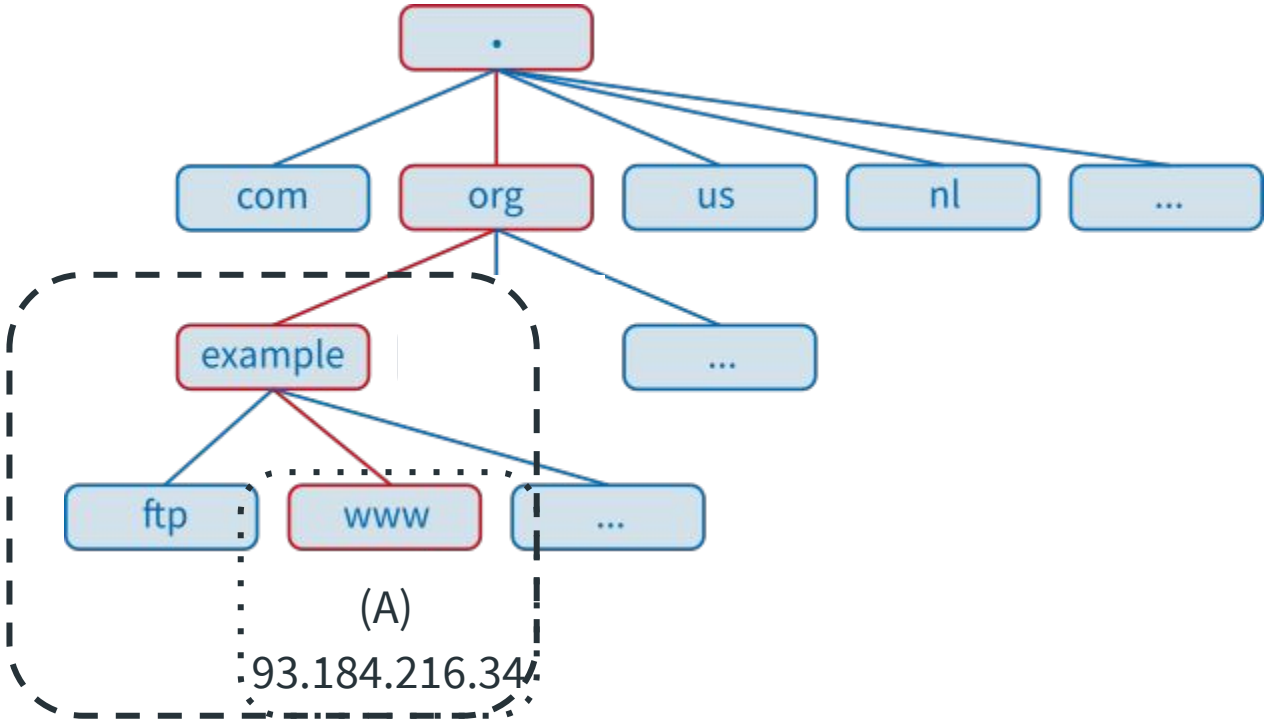
NS - Authoritative Name Server

MX - Mail Exchange

DNS RESOURCE RECORD - WWW



DNS ZONE - EXAMPLE.ORG.



Terminology

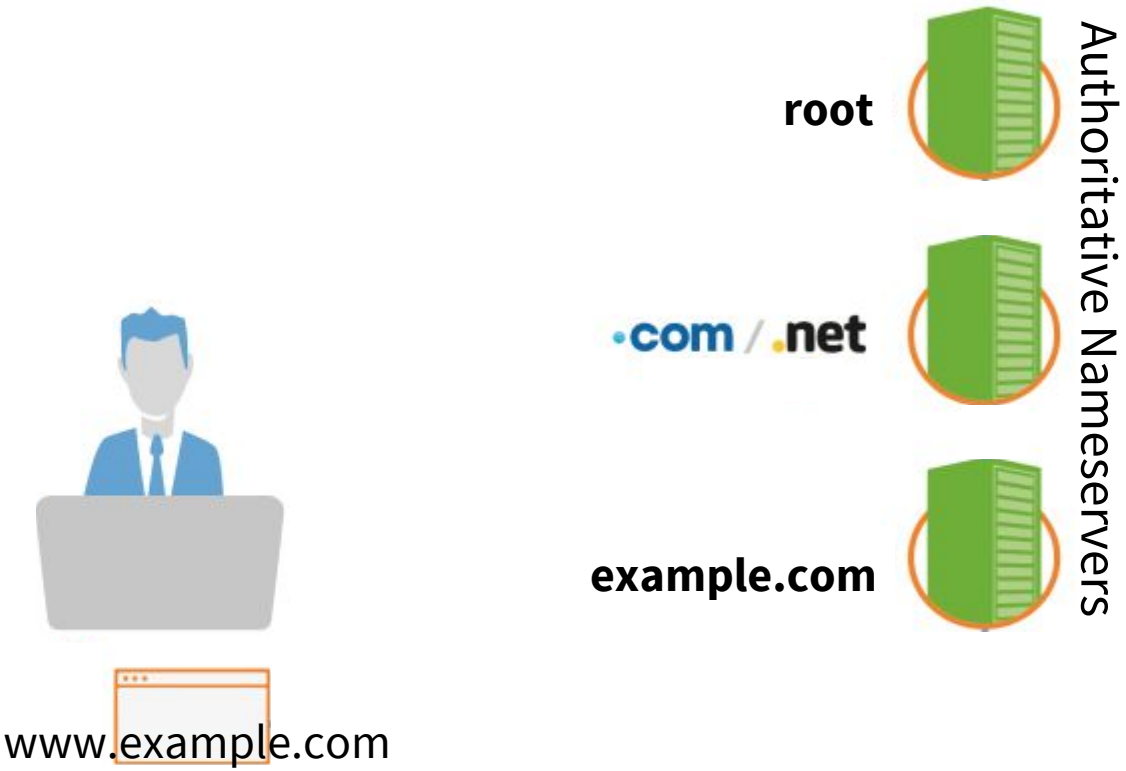
A **Nameserver (NS)** maintains a directory of domain names to their IP addresses.

Nameservers are
The Internet's “phone books”

Using the Phone Book

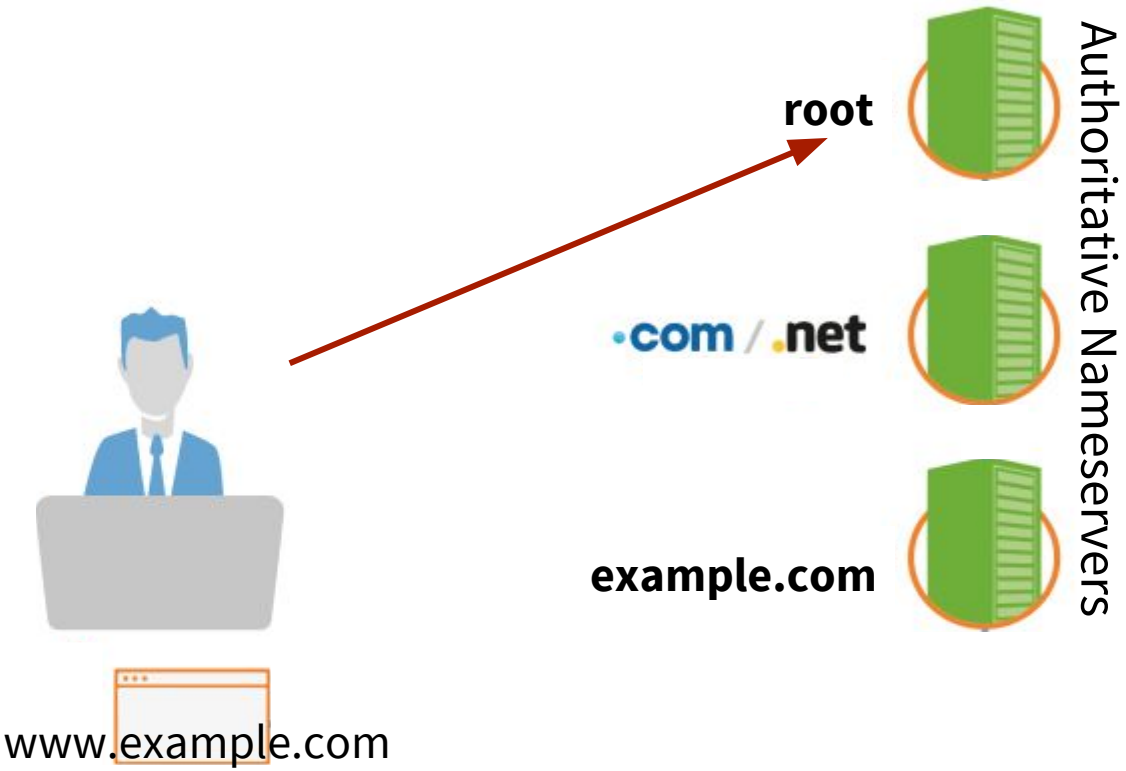
How DNS translates

DNS Lookup



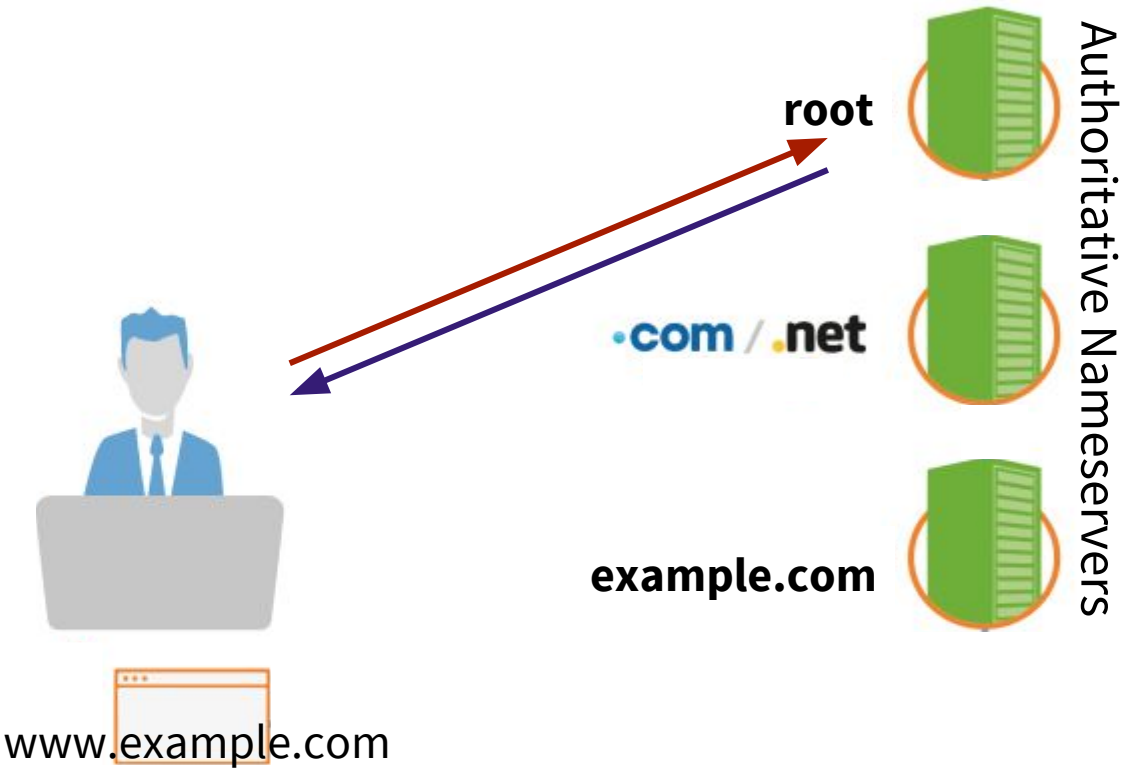
How does my computer find www.example.com?

DNS Lookup



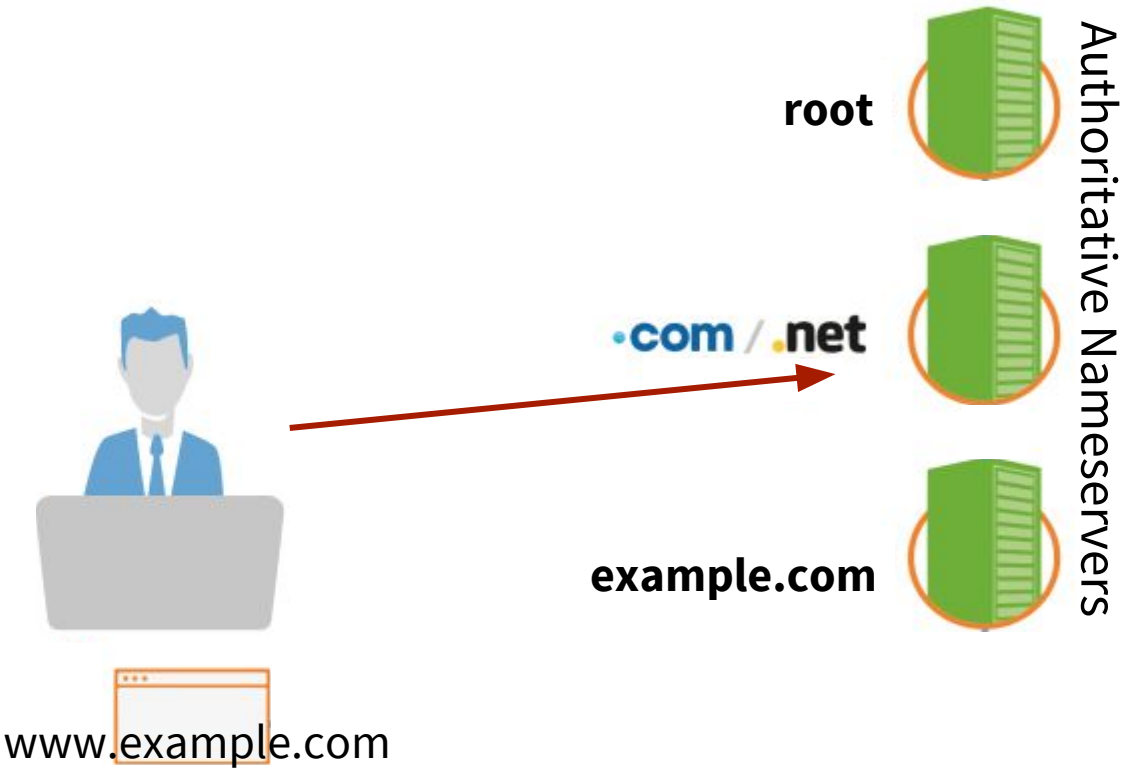
Where is www.example.com?

DNS Lookup



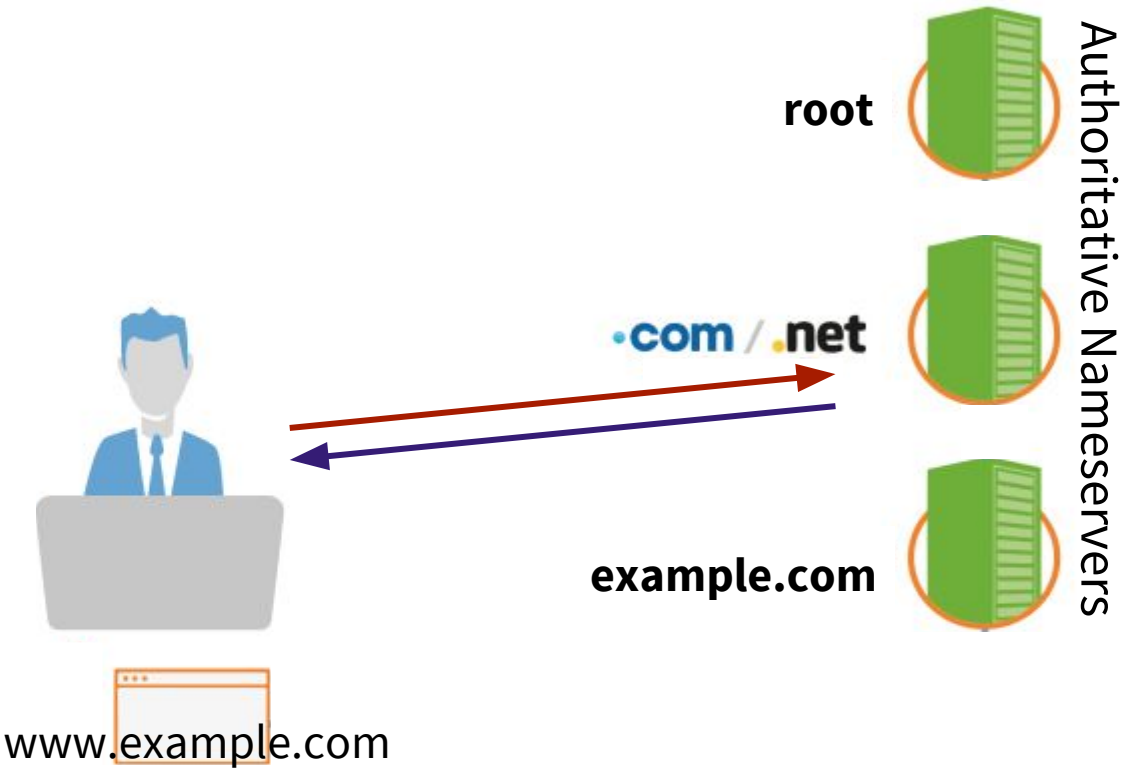
Go ask .com's nameserver (NS)

DNS Lookup



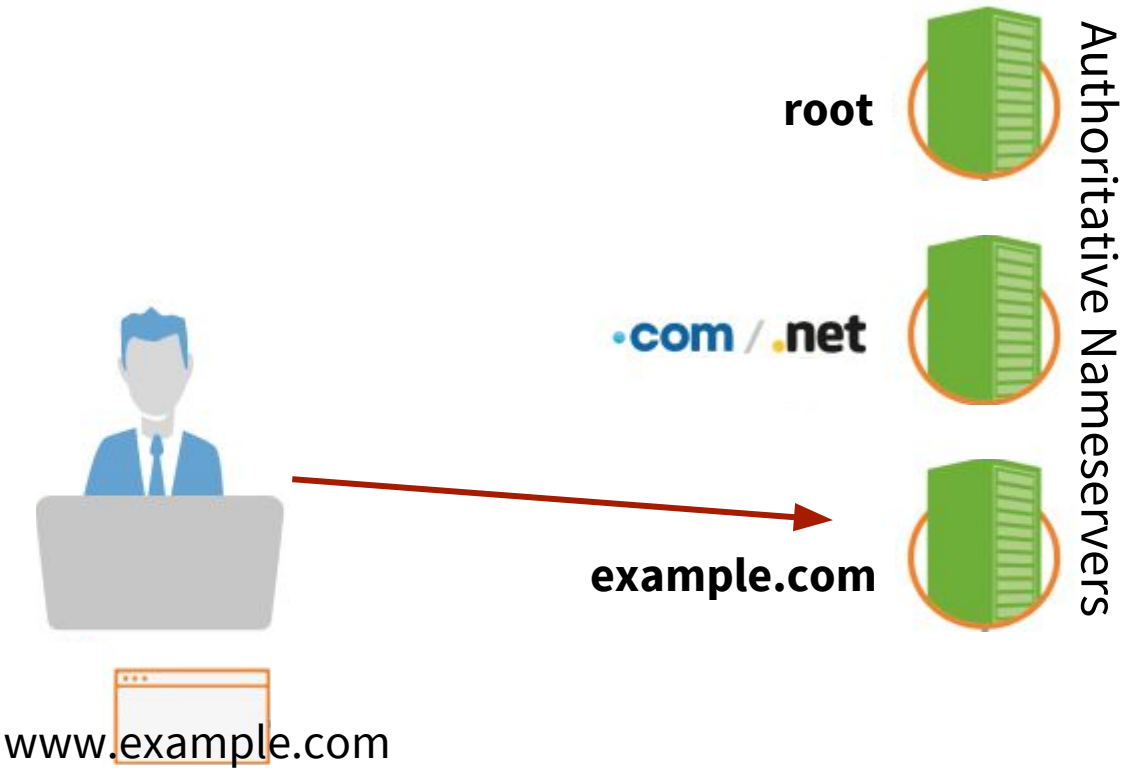
Where is www.example.com?

DNS Lookup



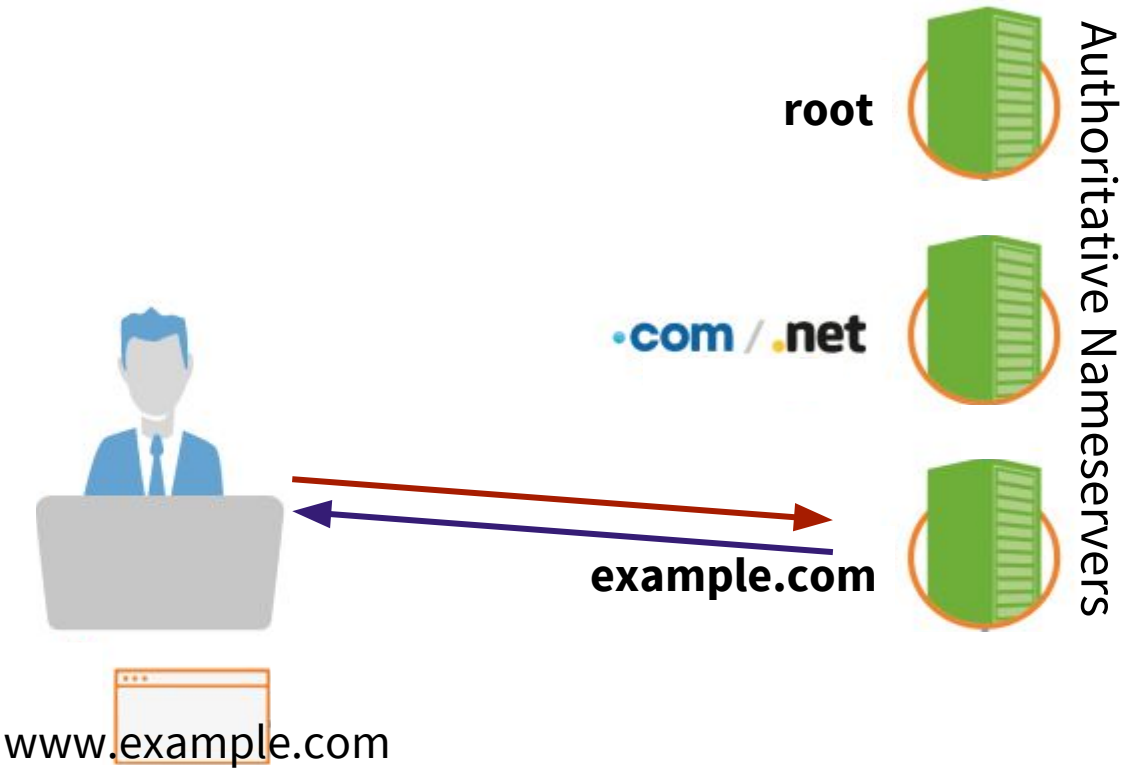
Go ask example.com's nameserver (NS)

DNS Lookup



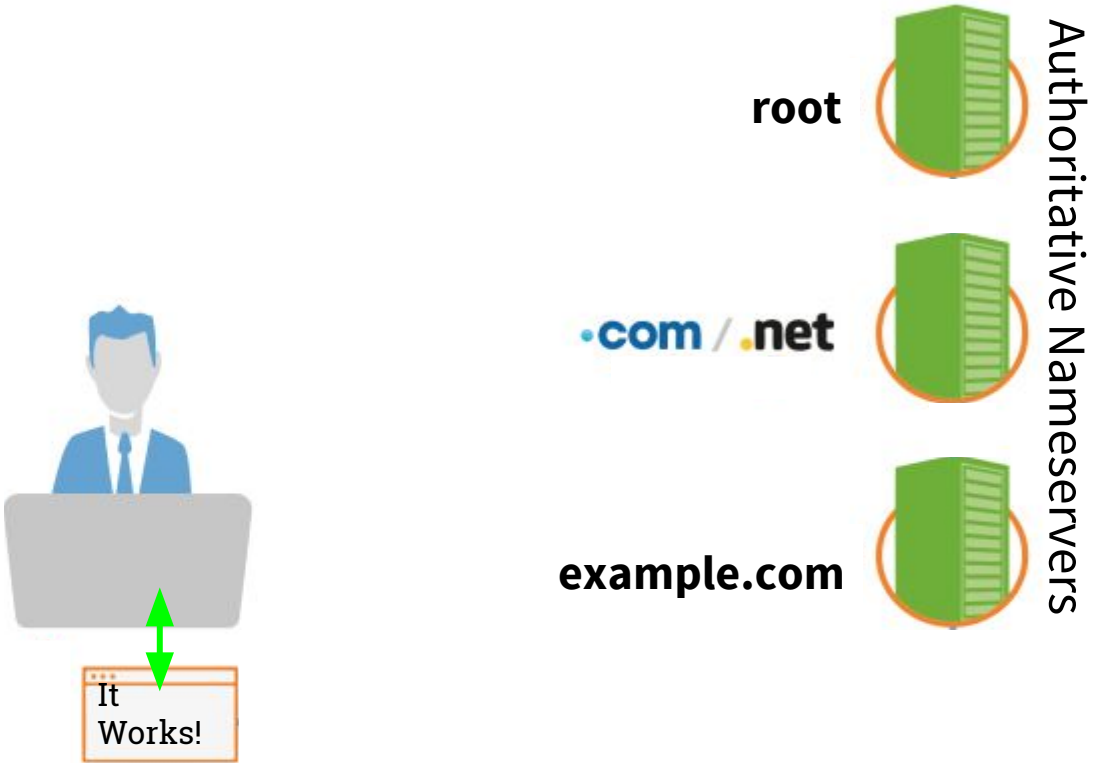
Where is www.example.com?

DNS Lookup



www.example.com is at
93.184.216.34 (A)

Site Found



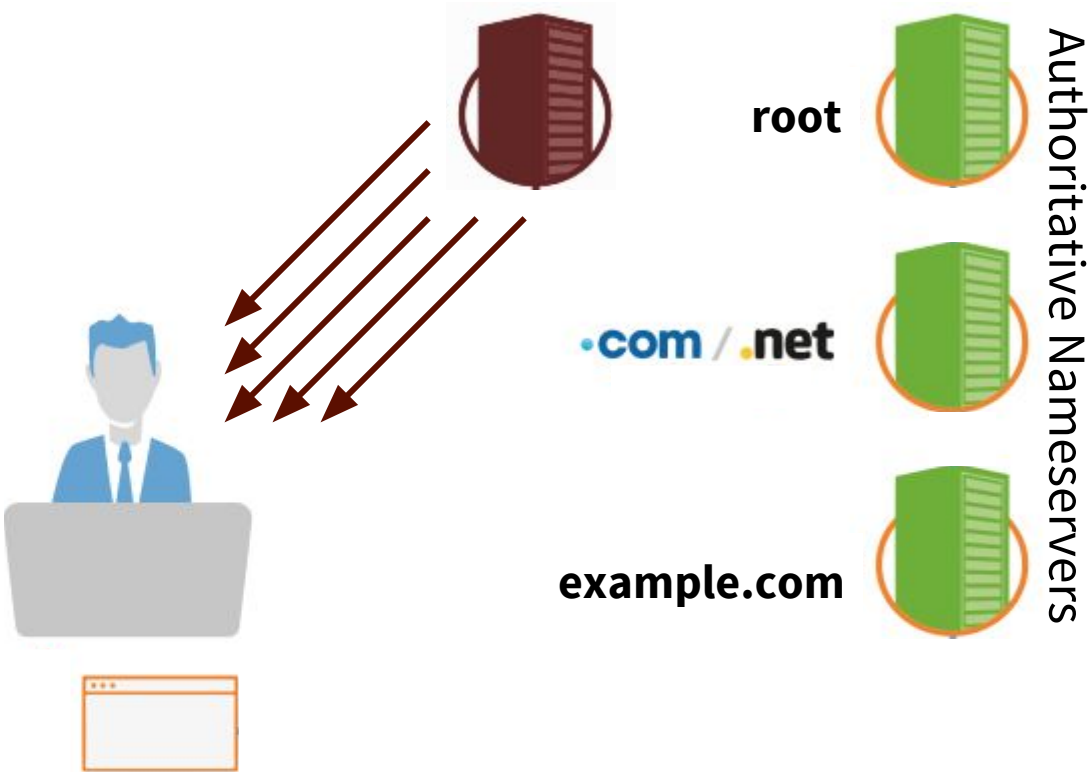
Communicate with
www.example.com!

Exploits

DNS Hijacking, Spoofing, and Cache Poisoning

- Kaminsky Bug
- Rogue DNS Servers
- MITM
- Direct Manipulation (State, ISP, etc)
- Route Hijacking

DNS Poisoning



Flood with fake answers

DNS EXPLOITED

2007 - 2011 - DNSChanger/RSPlug

2011 - Brazilian ISPs fall victim DNS cache poisoning

2014 - Turkey intercepts Google’s public DNS service

SSL/TLS Can't Save You

And the CA problem

SSL/TLS

SSL (Secure Sockets Layer) establishes an encrypted connection between a web server and a browser.

SSL/TLS matches the the certificate to the DNS name, not if you've been sent to the correct site.

SSL/TLS CERTIFICATE AUTHORITIES

SSL/TLS uses certificates obtained from a 3rd party called a CA (Certificate Authority).

- Too many CAs
- A CA can delegate trust subordinate certifications authorities
- Any CA can issue certificates for any entity on the Internet

WHEN SSL/TLS FAILS

- Comodo and DigiNotar compromise results in issuing of fraudulent certificates
- Symantec issued rogue Google certificates
- Microsoft, Dell, and D-Link leaked private keys

We need to secure DNS for a secure Internet.

DNSSEC

Tamper-proof DNS

Domain Name System Security Extensions

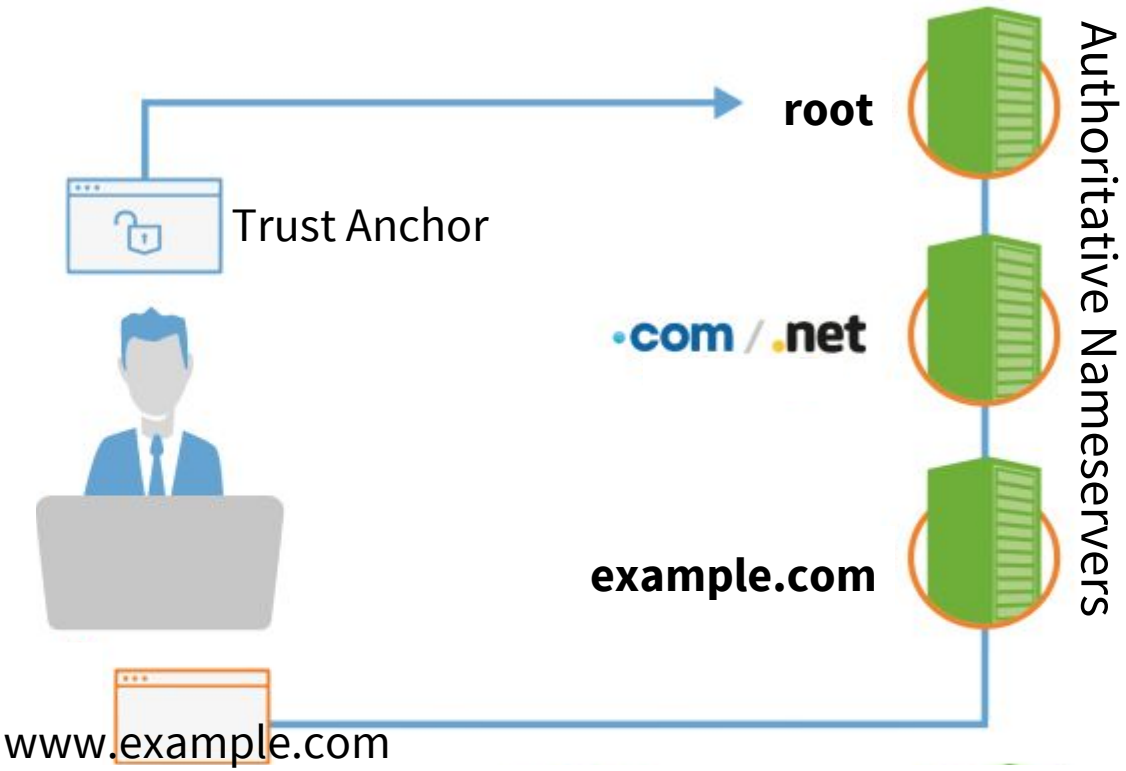
DNSSEC

- Protects users
- Strengthens trust in the Internet
- Backwards compatible

DNSSEC Authenticates

1. DNS data originated from a legitimate sender
2. Data was not tampered in transit
3. Nonexistent data does not exist

Chain of Trust

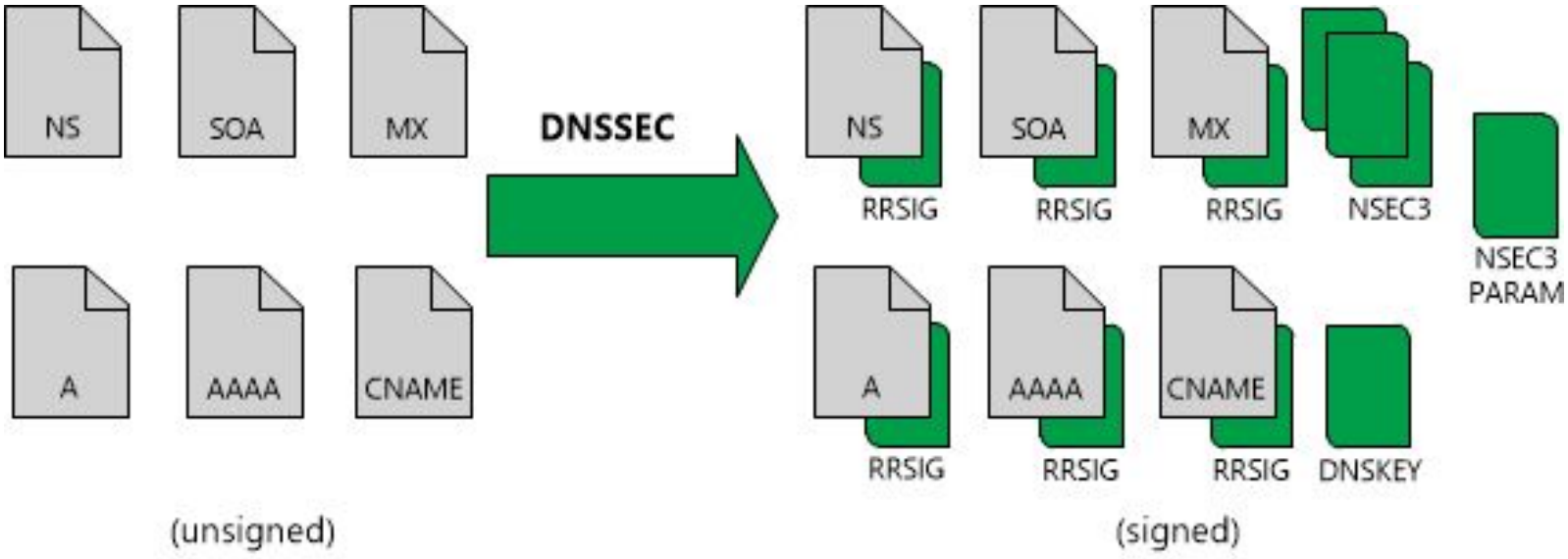


DNSSEC IS NOT

DNSSEC does not:

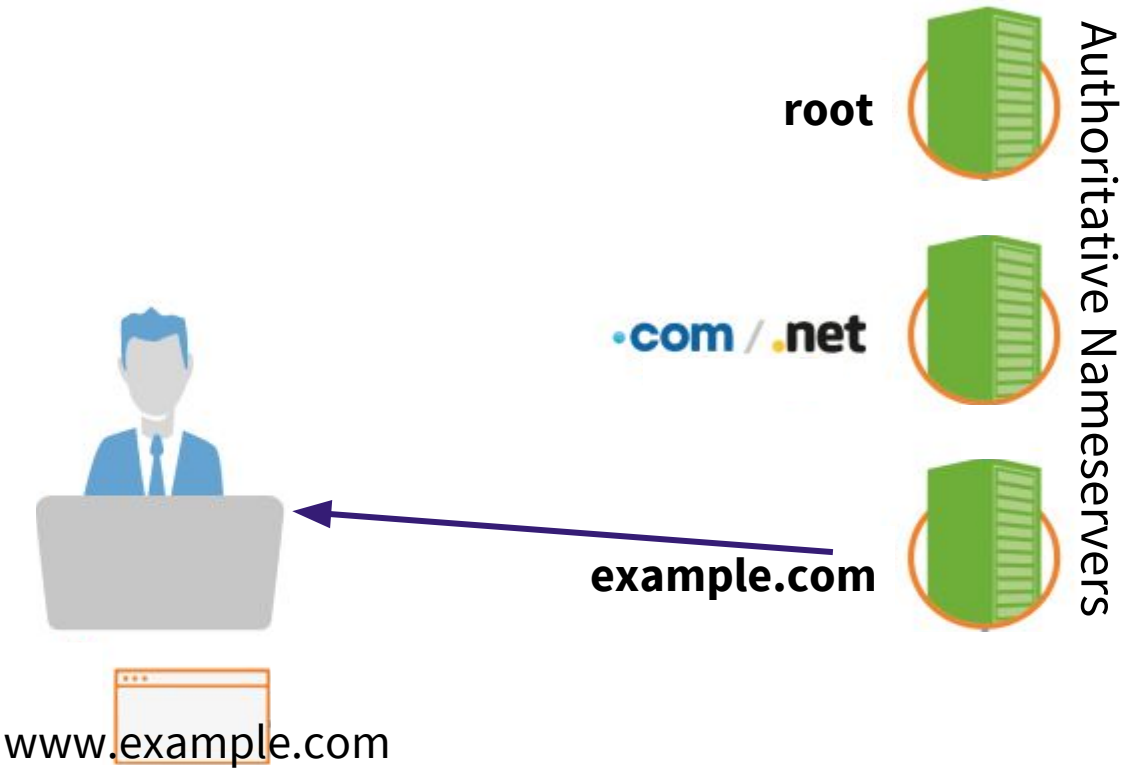
- Provide confidentiality
- Guarantee availability
- Protect against compromised nameservers

Signed Zone



RRSIG contains the cryptographic signature of the data.

DNSSEC Lookup



www.example.com is at
93.184.216.34 (A) + Signature of A (RRSIG)

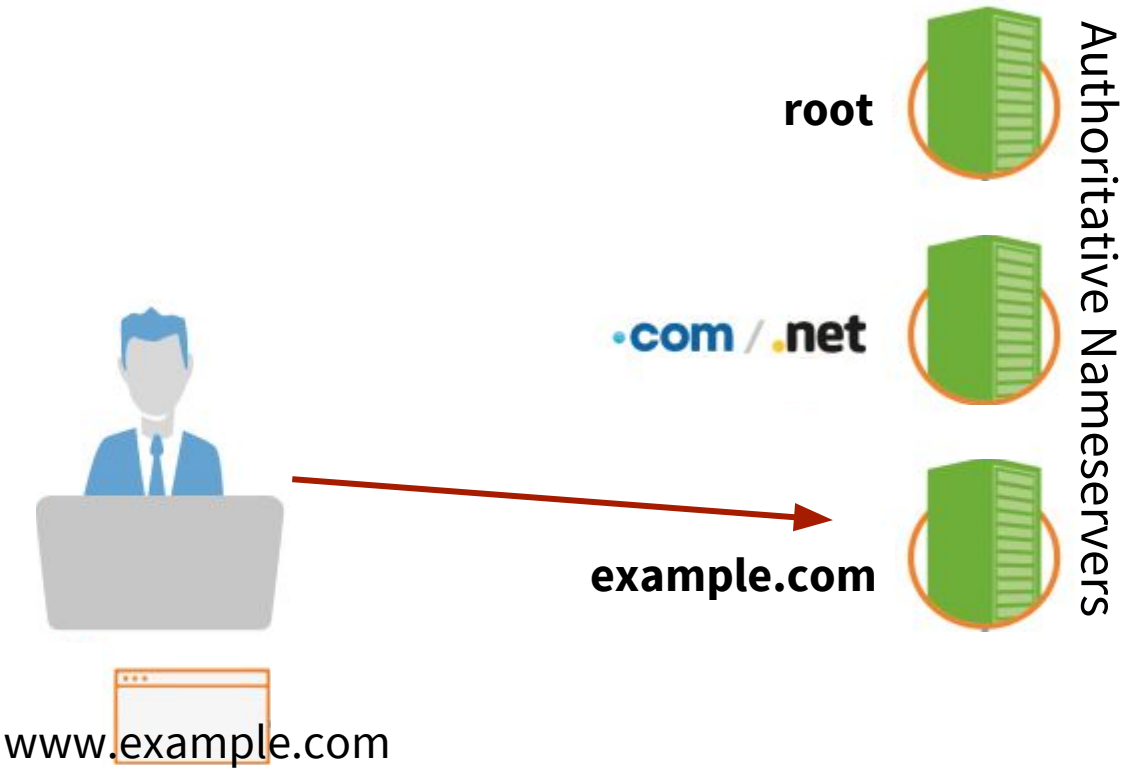
DNSSEC RESOURCE RECORDS

- **DNSKEY**
  DNS Public Key

- **RRSIG**
  Resource Record Signature

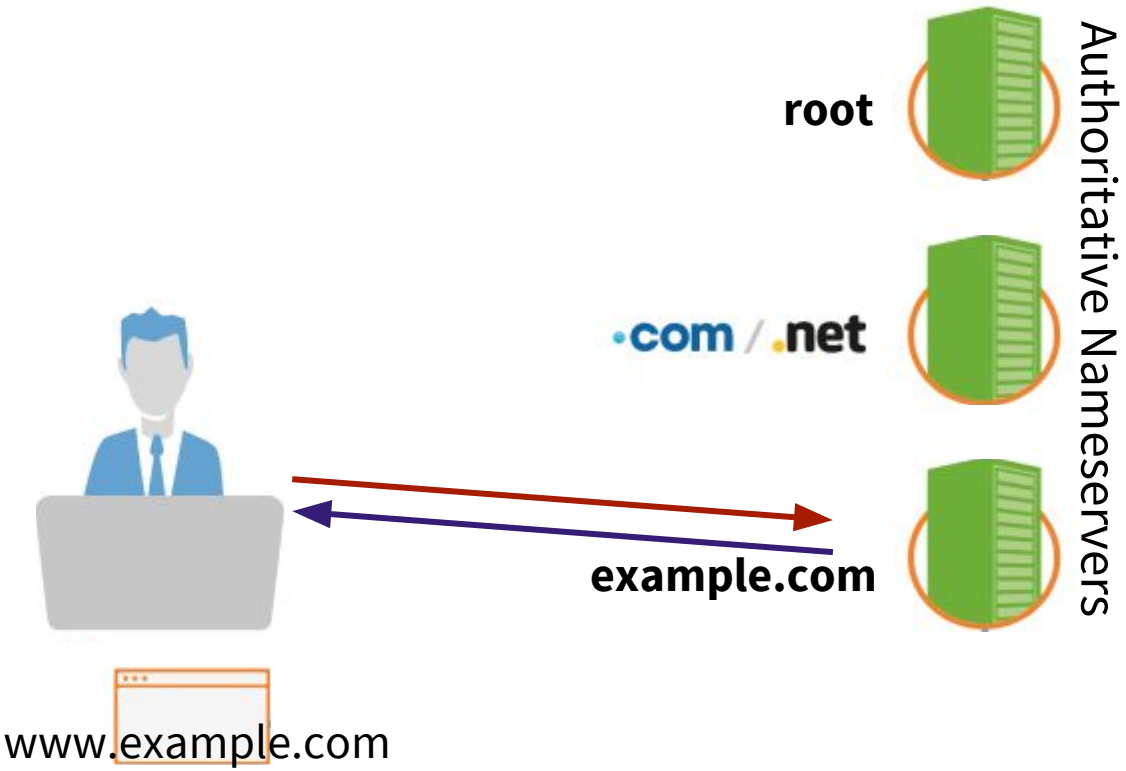
- **DS**
  Delegation Signer

DNSSEC Validation



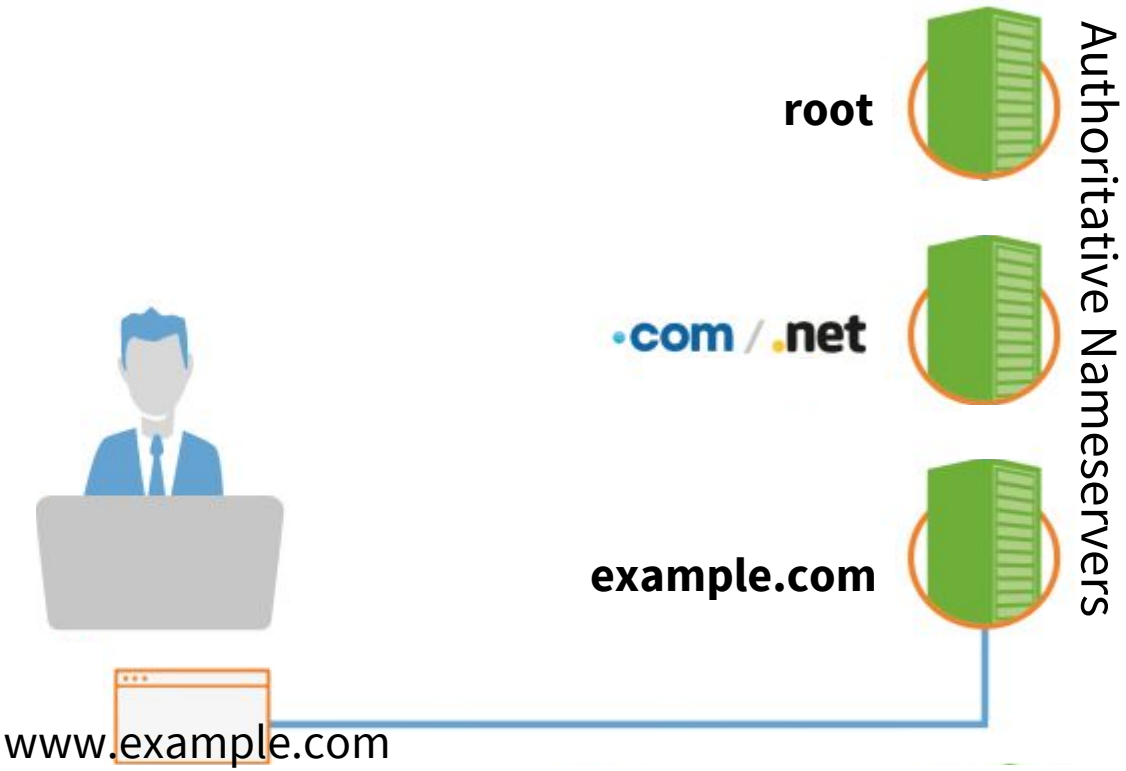
What is the public key for example.com?

DNSSEC Validation



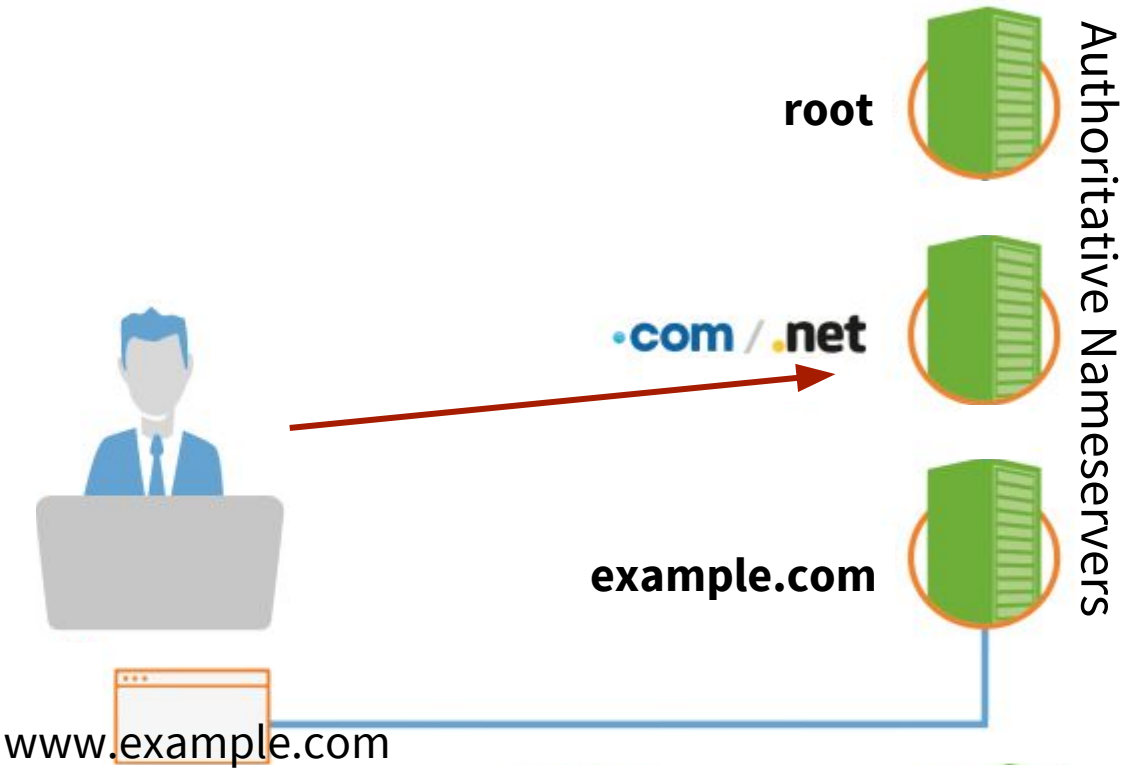
example.com's public key (DNSKEY)

DNSSEC Validation



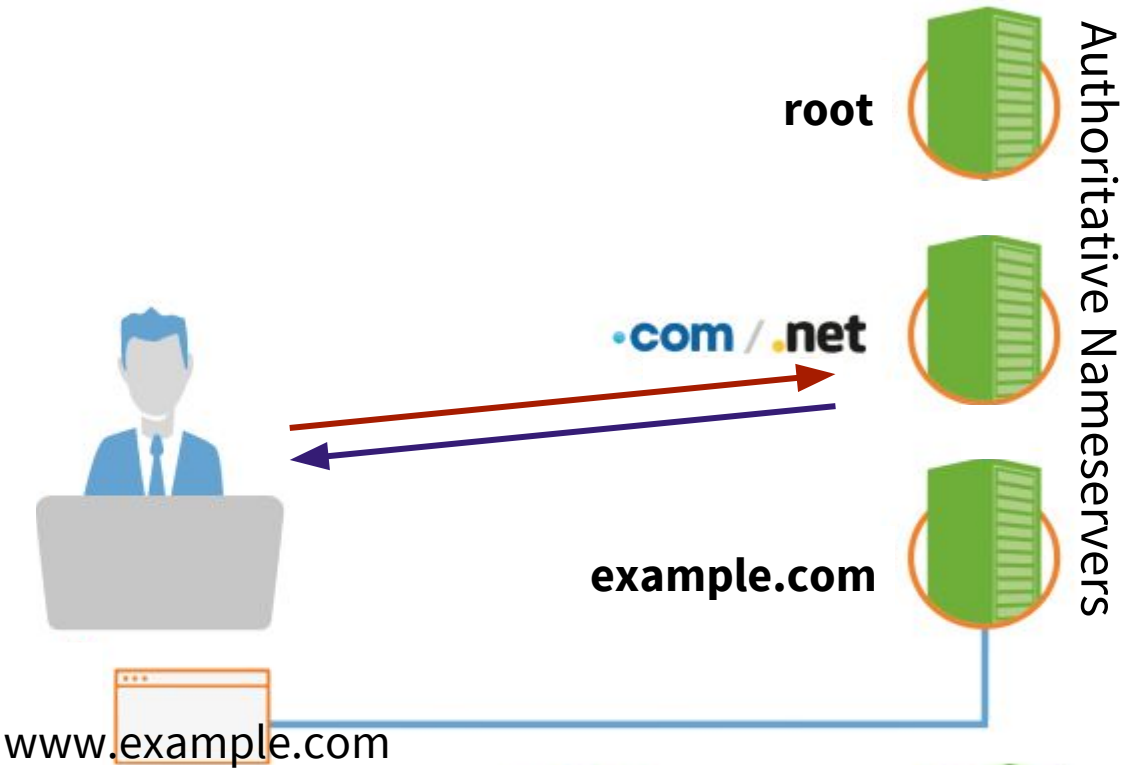
Signature (RRSIG) of www.example.com validated

DNSSEC Validation



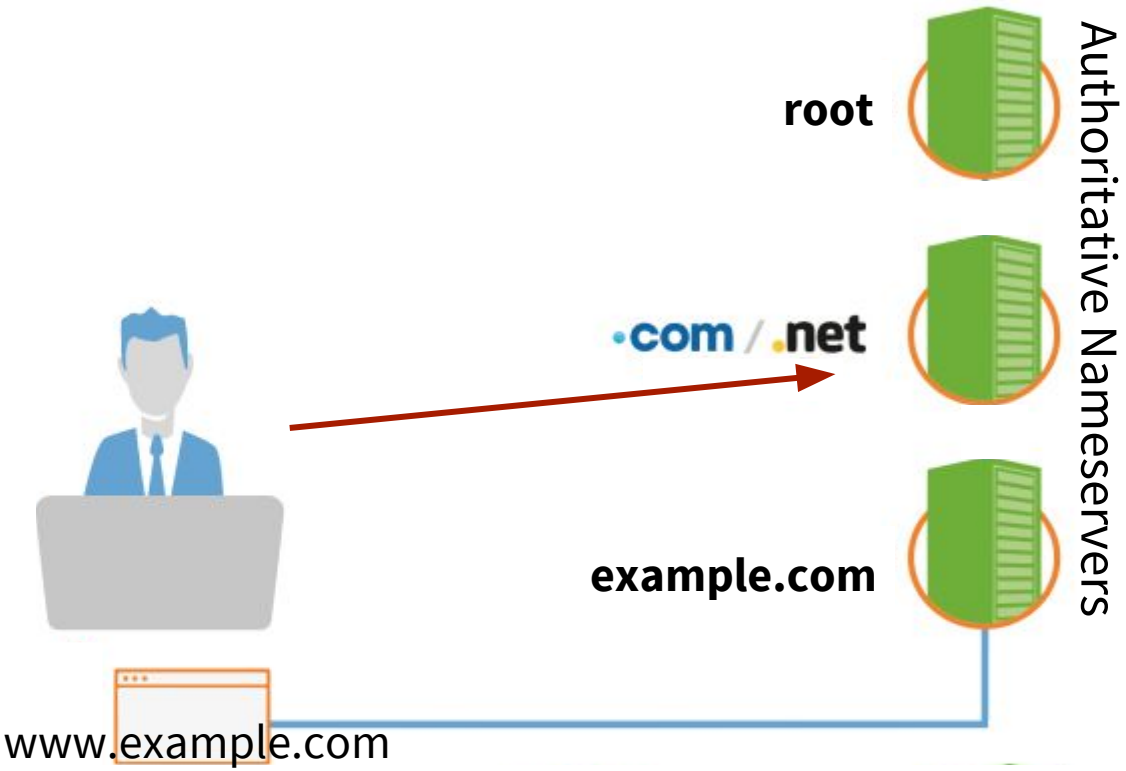
What is the hash of example.com's public key record?

DNSSEC Validation



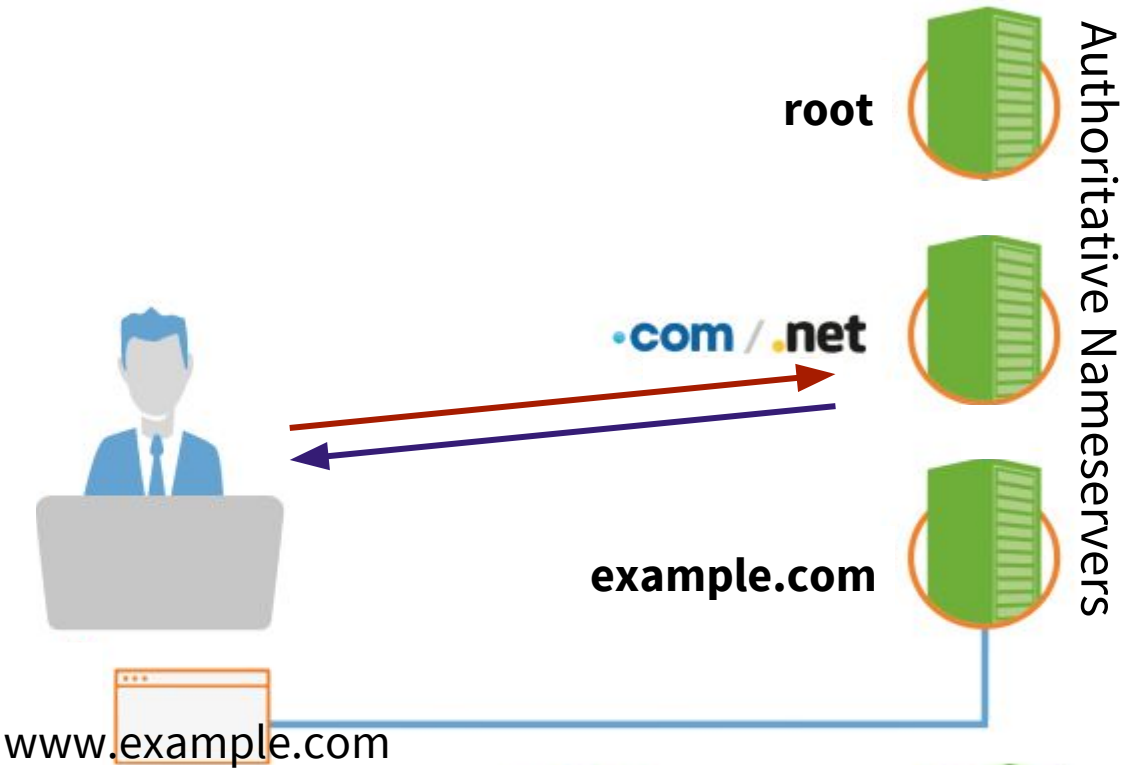
Hash of example.com's public key record (DS) and hash's signature (RRSIG)

DNSSEC Validation



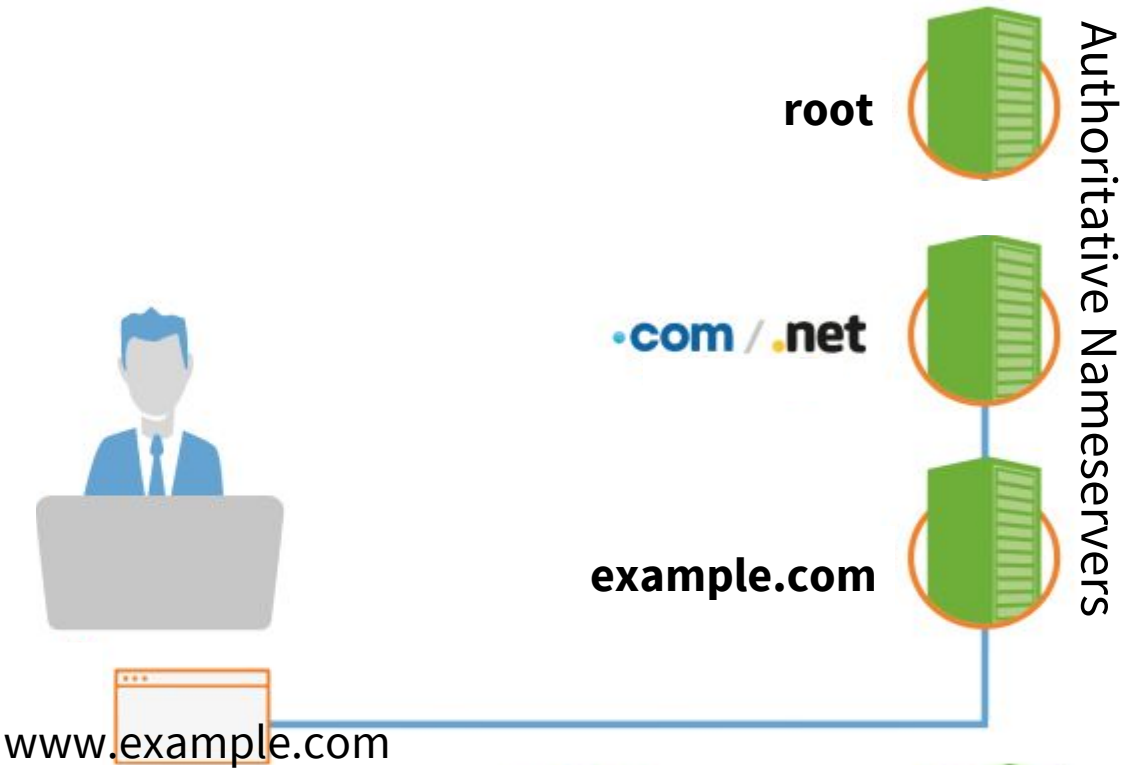
What is the public key for .com?

DNSSEC Validation



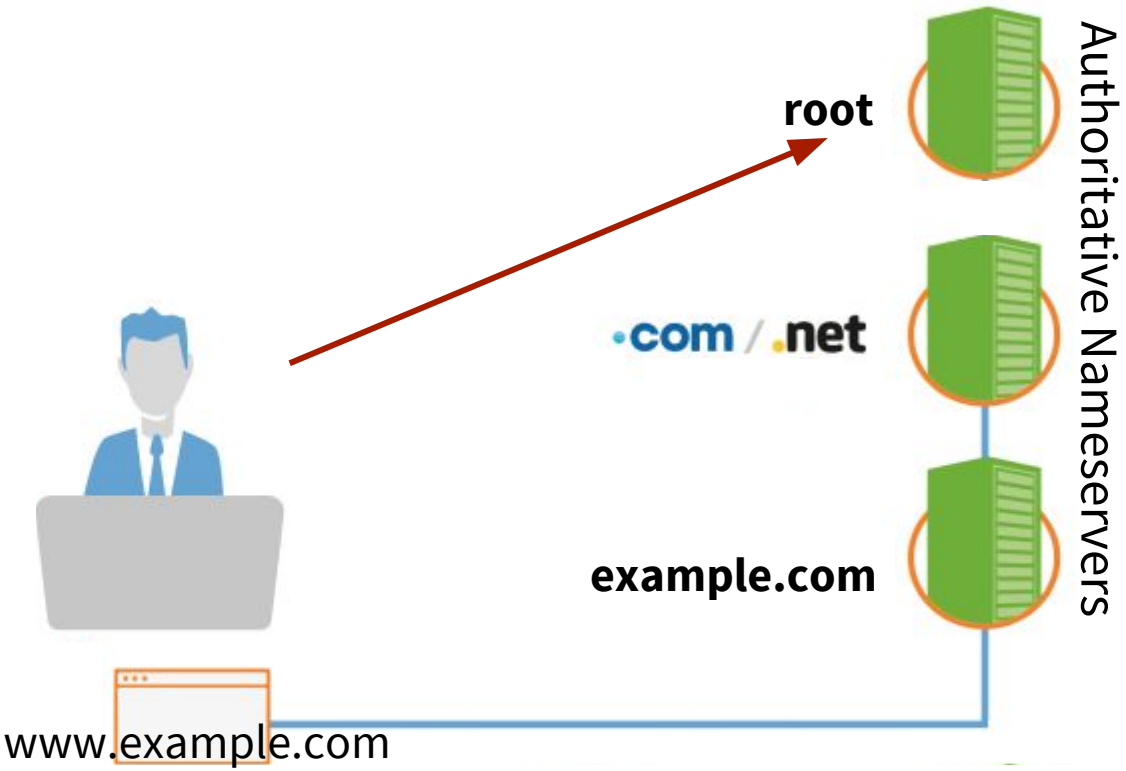
Public key for .com
(DNSKEY)

DNSSEC Validation



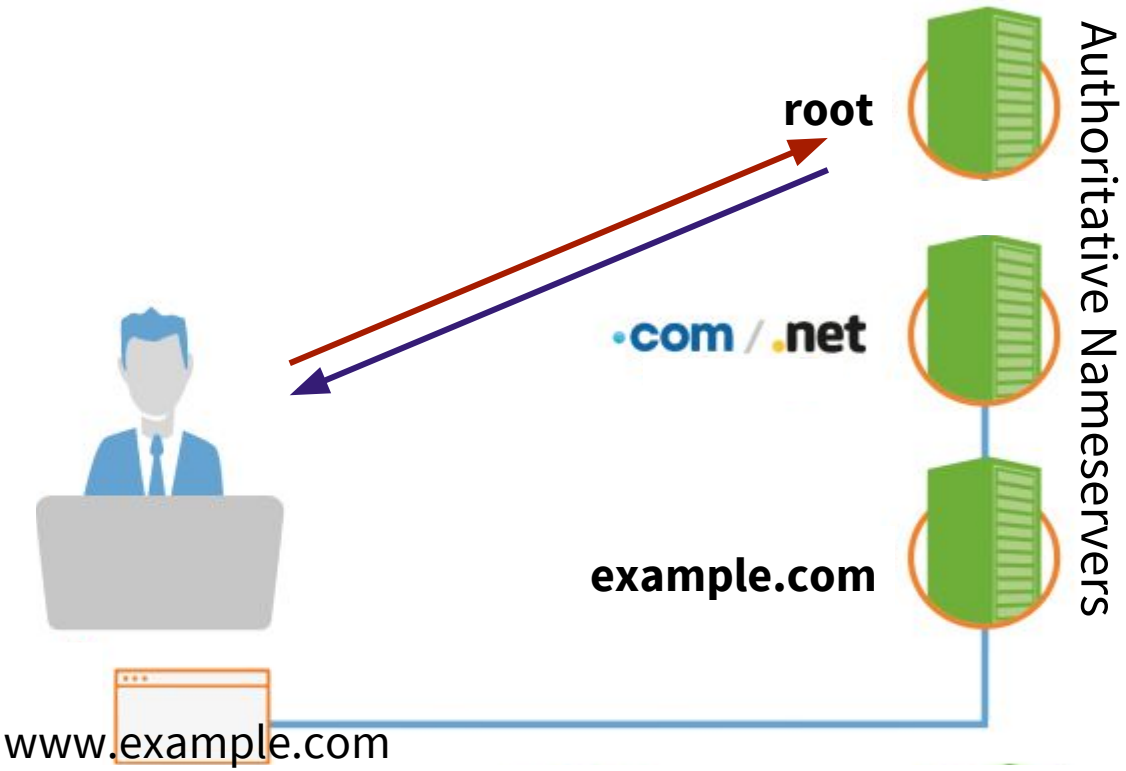
example.com's public key validated

DNSSEC Validation



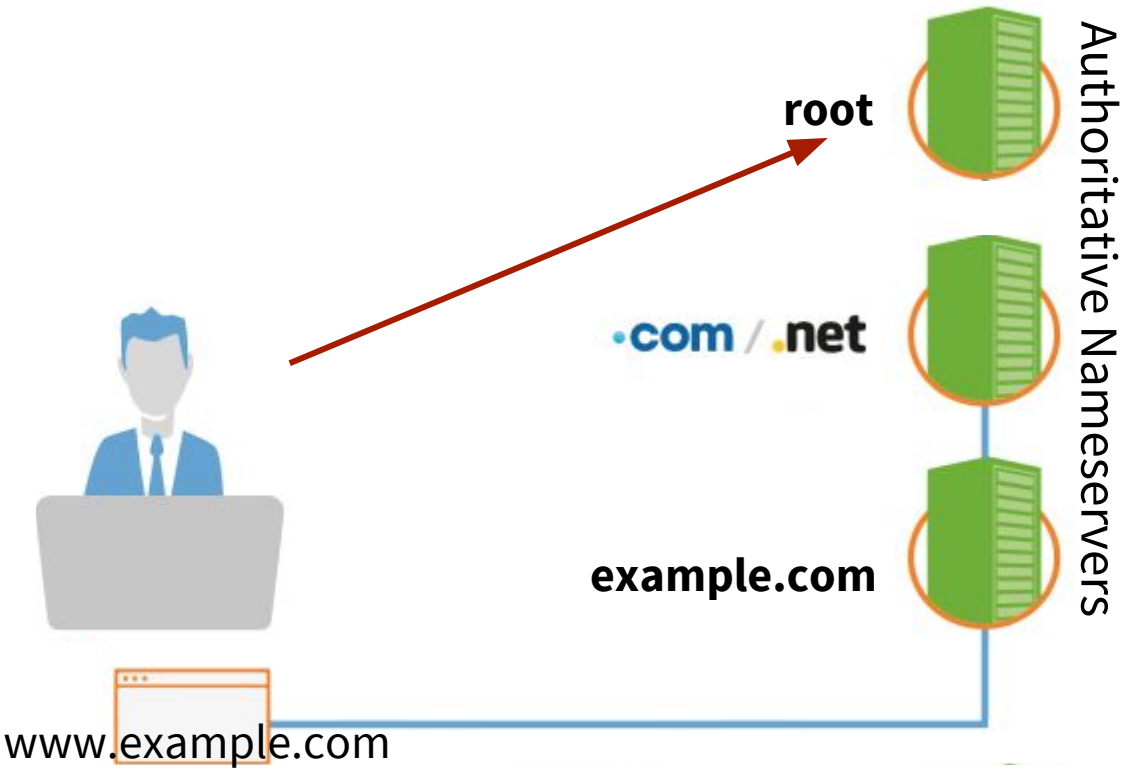
What is the hash of
.com's public key?

DNSSEC Validation



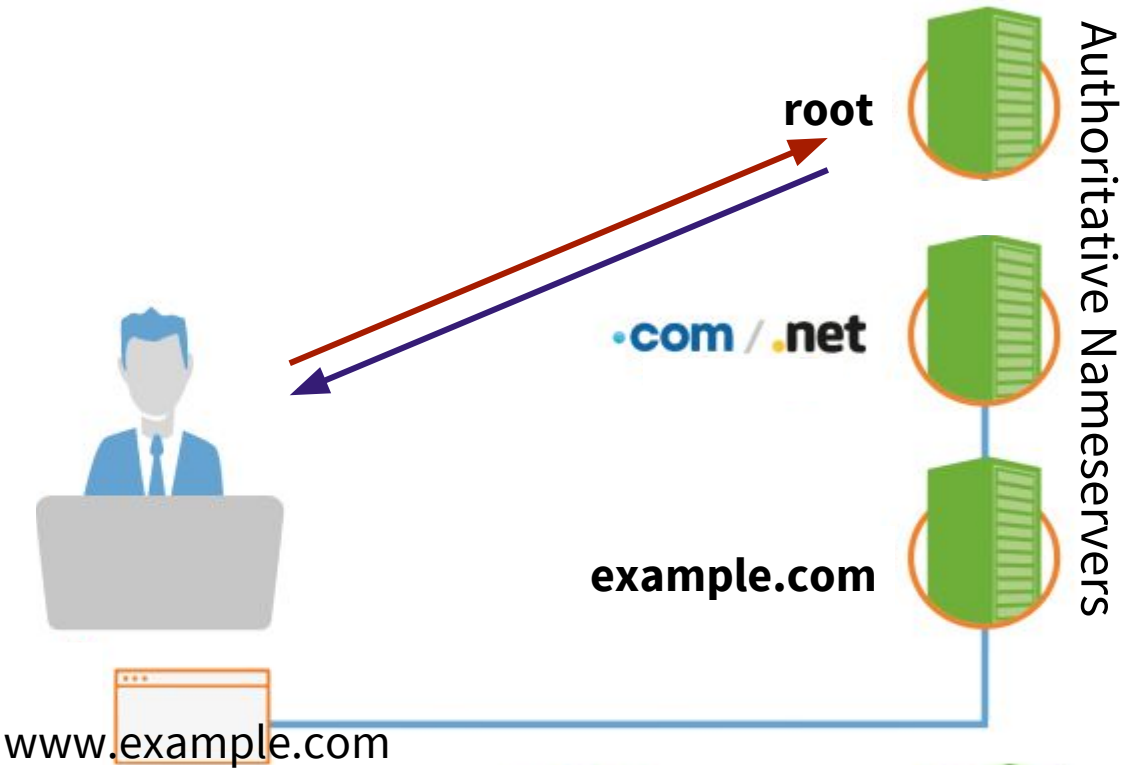
Hash of .com's
public key (DS) + signature (RRSIG)

DNSSEC Validation



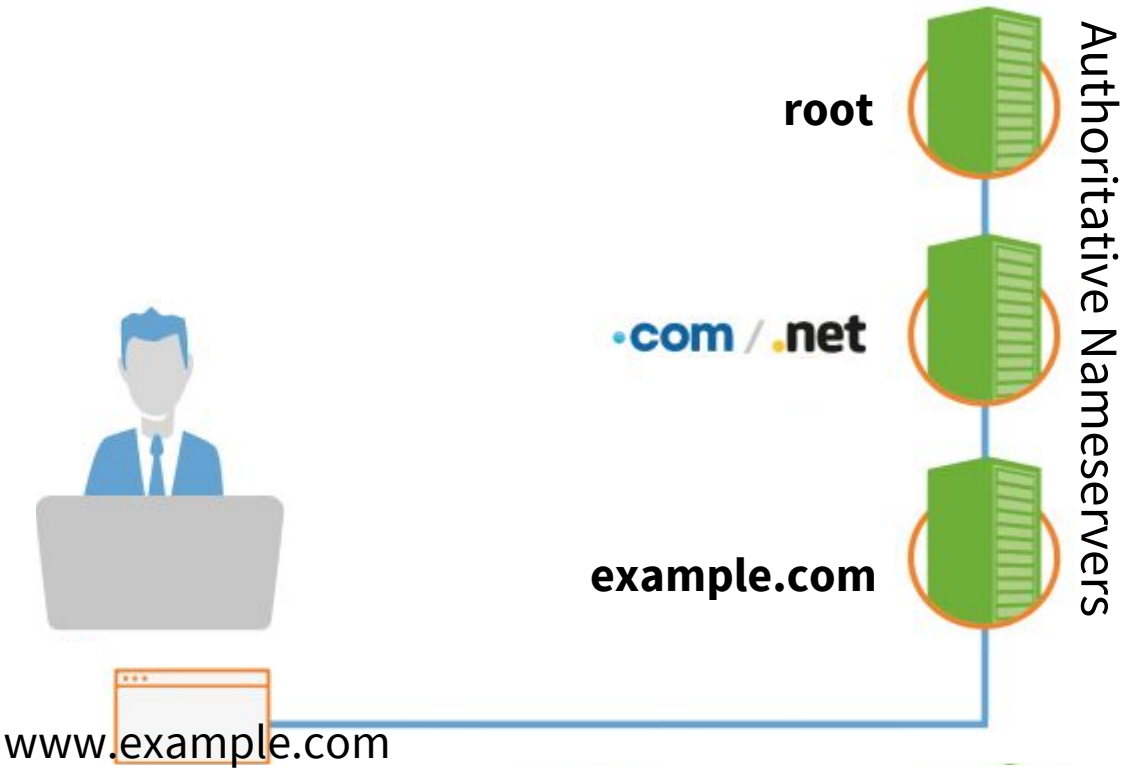
What is the public key for root?

DNSSEC Validation



Public key for root
(DNSKEY)

DNS Lookup



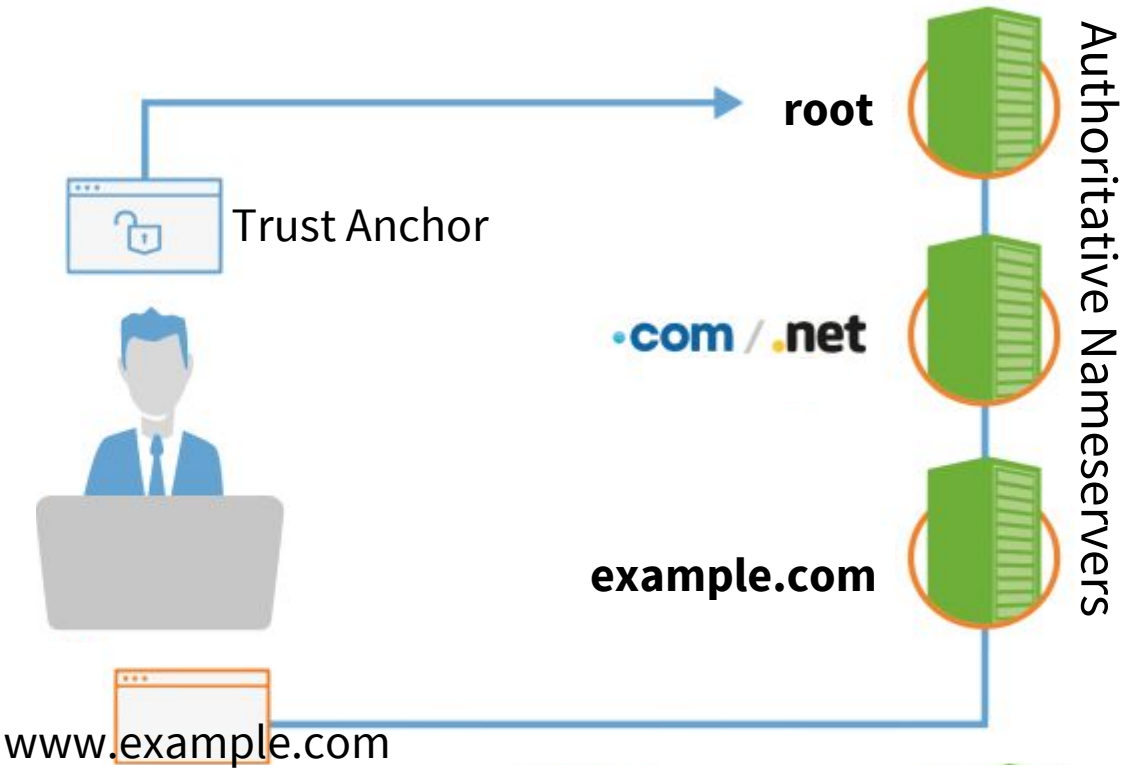
.com's public key validated

DNSSEC - Trust Anchors

Trust anchor to validate root

- Authoritative key
- Starting point in chain of trust.

Chain of Trust



Trust anchor validates root's public key

AUTHENTICATED DENIAL OF EXISTENCE

- Validates that data does not exists
- Prevents MITM attack

DNSSEC Resource Records

- **NSEC (Next Secure)**

  Points to the next name in the zone, if record queried does not exist.

Zone-Walking
A side effect allows discovery of zone content

DNSSEC Resource Records

- **NSEC3** impedes zone-walking by using hashes.
- **NSEC5** is being being discussed to solve zone-walking issue.

In DNS We Trust

Cryptographic signatures
+ Chain-of-Trust

DNS DATA IS AUTHENTICATED

- **Origin Authenticity**
  Data originated from a legitimate sender.
- **Data Integrity**
  Validation data was not modified in transit.
- **Authenticated Denial of Existence**
  Validation of absence of data,
  when it does not exist

DNS, A Trusted Database

DNS is the most successful distributed database

DNSSEC transforms the DNS into an authenticated directory of information

TRUSTING DNS DATA

We can trust:

- **DKIM / SFP (TXT)** - For fighting spam
- **MX** - Mail Exchange
- **SRV** - Service Discovery (VoIP and XMPP)
- **NAPTR** - Name Authority Pointer (Internet telephony)

TRUSTING DNS with KEYS, CERTS, AND FINGERPRINTS

Confidence with data:

- **IPSECKEY** - IPSec Key Storage (VPN)
- **TSIG** - Transaction Signature for zone updates
- **SSHFP** - Secure Shell Fingerprints

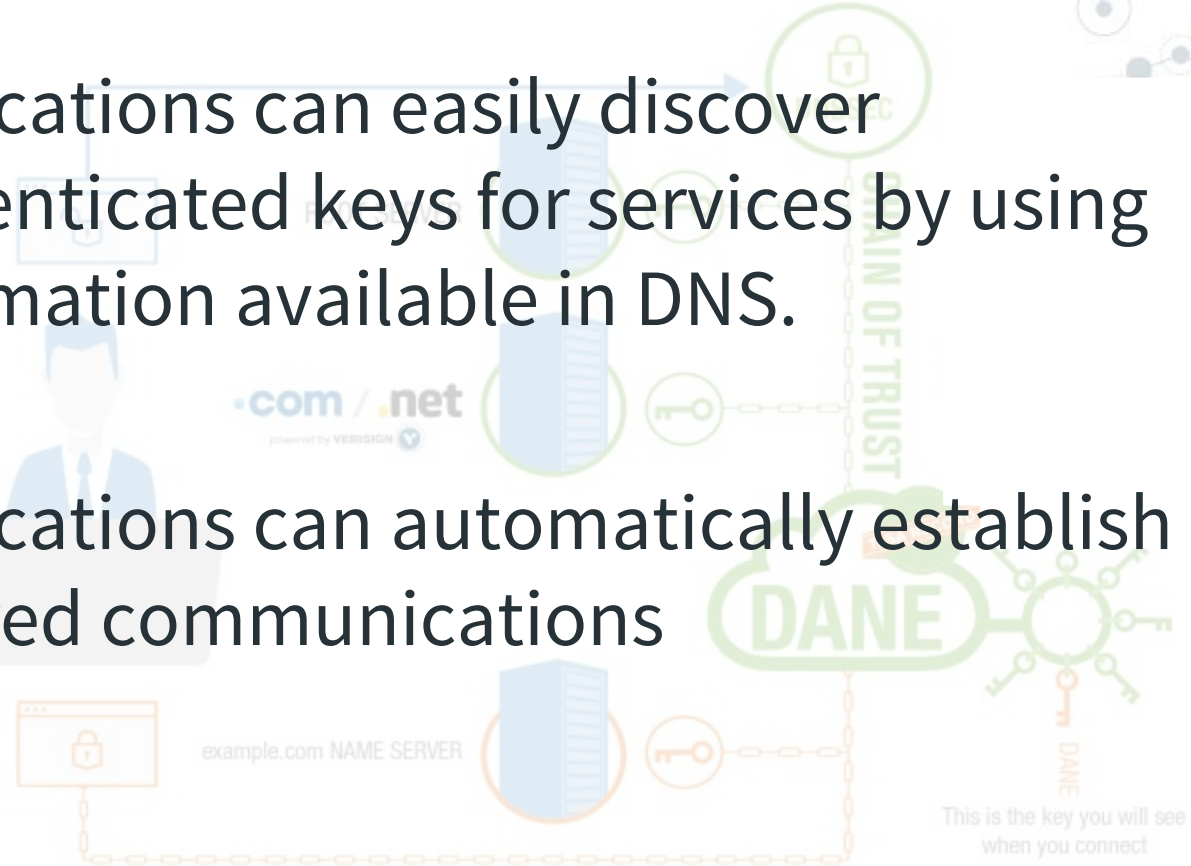
DANE

Secure Key Learning

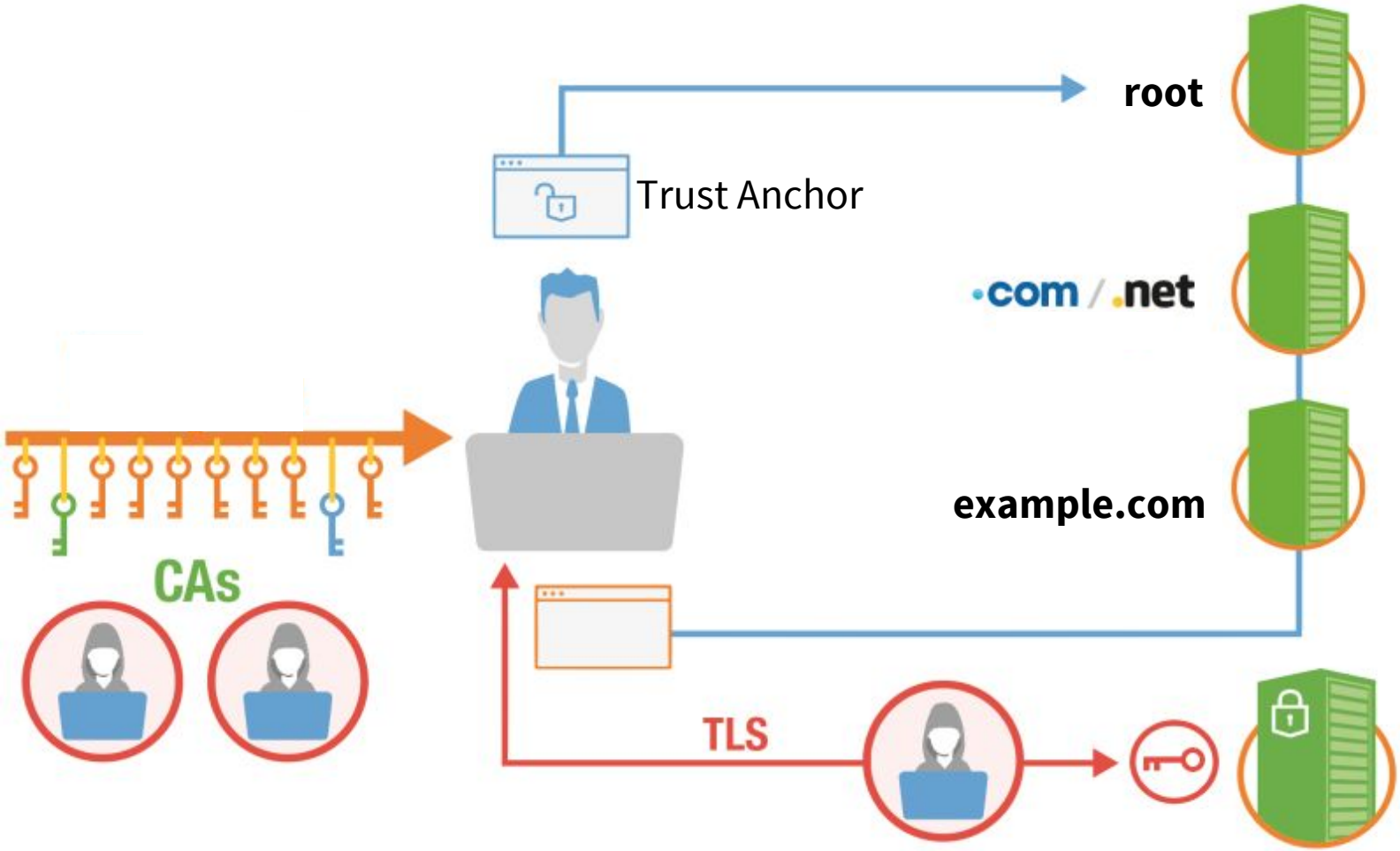
DNS-based Authentication of Named Entities

DANE

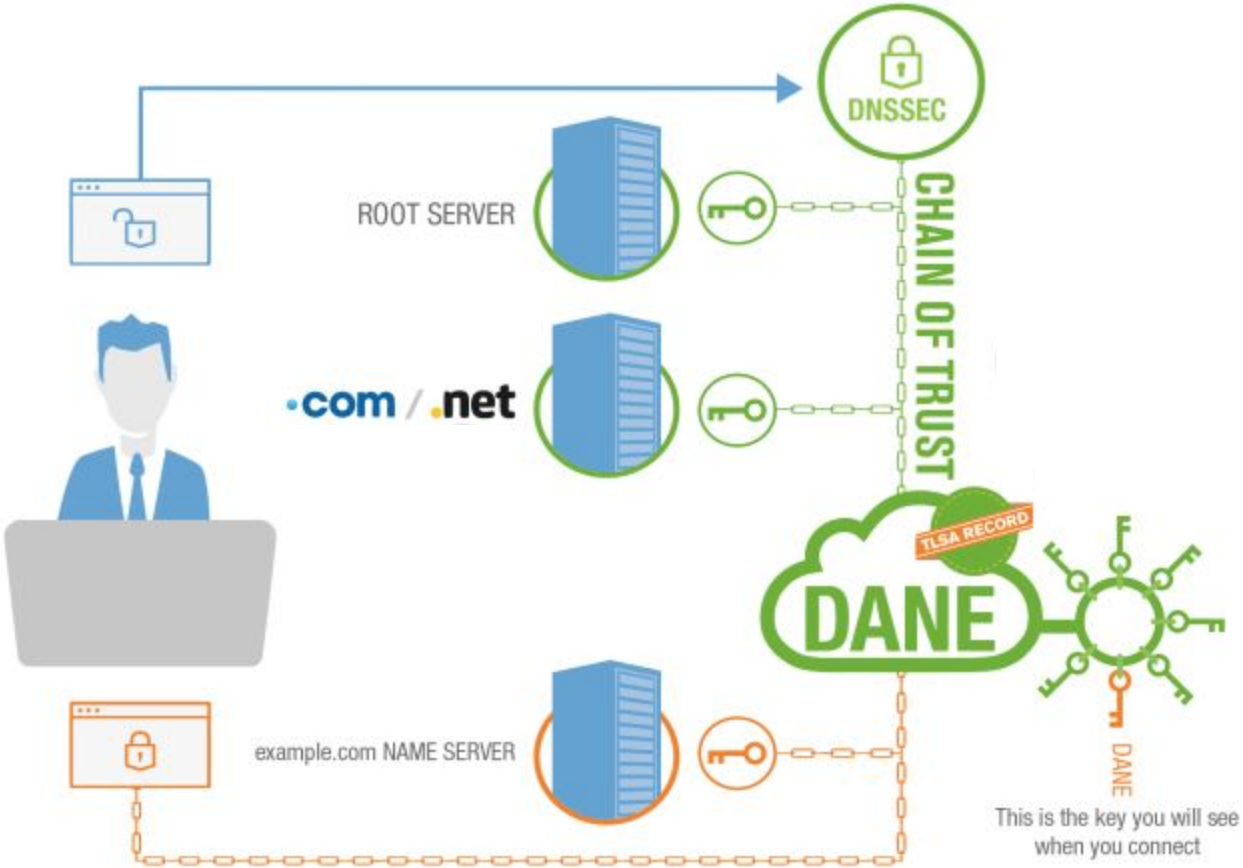
- Applications can easily discover authenticated keys for services by using information available in DNS.
- Applications can automatically establish secured communications



Current SSL/TLS System



TLS with DANE



TLS In DNS

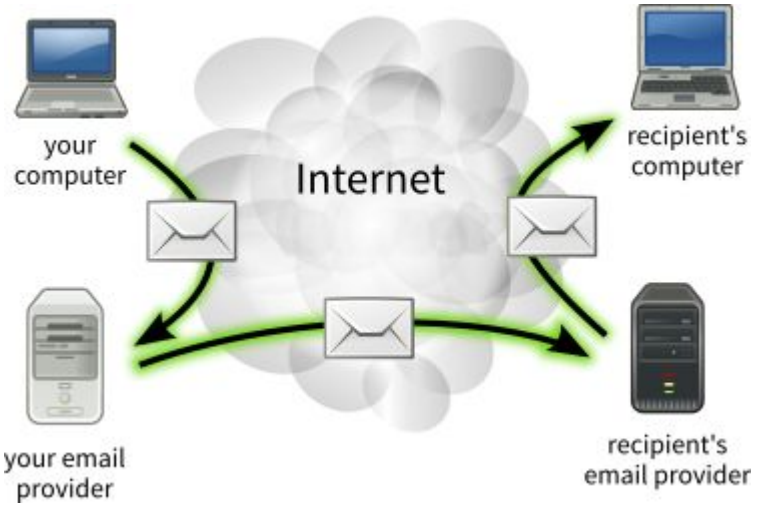
TLSA - TLS associations

- Stores a certificate or key for TLS
- Can work in conjunction with certificate authorities

TLSA and EMAIL

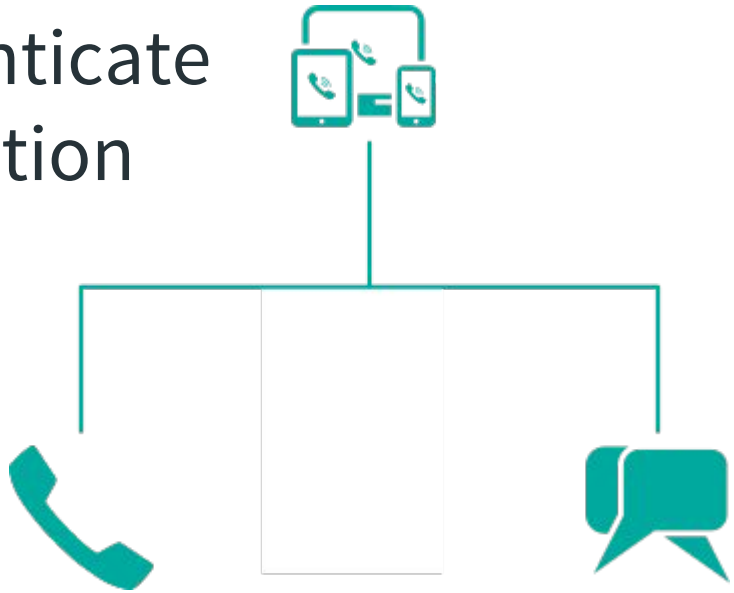
STARTTLS = SMTP + TLS

- STARTTLS is susceptible to MITM, Downgrade, and DNS attacks.
- DANE can authenticate and enforce TLS for the SMTP connection



TLSA and UNIFIED COMMUNICATIONS

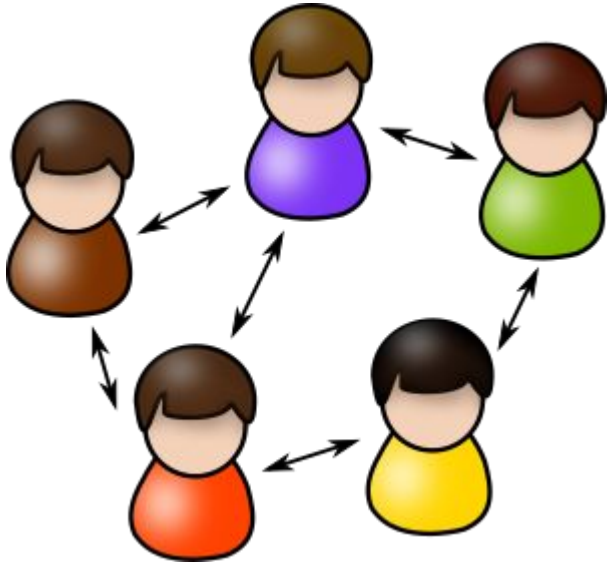
- DNSSEC is a great start, Validating NAPTR and SRV
- Instant Messaging: DANE can authenticate TLS to the XMPP server
- VoIP: DANE can authenticate TLS for the SIP connection




But Wait...
THERE'S MORE!!!

OPENPGPKEY

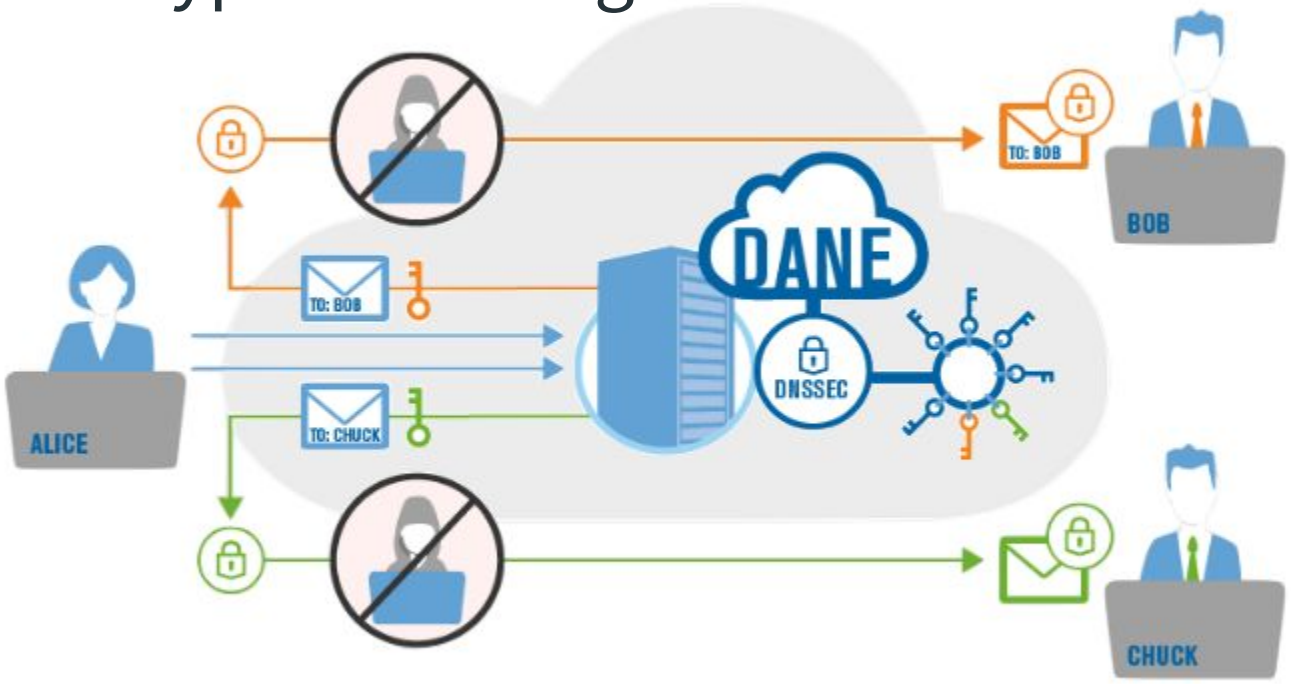
Discoverable PGP Public Key for encryption



DANE and EMAIL MESSAGES

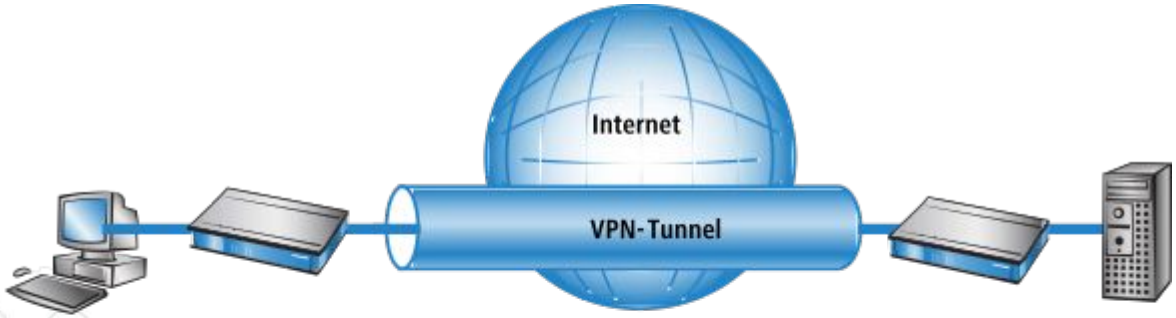
SMIMEA - S/MIME RR

Discoverable S/MIME key to digitally signed and encrypted messages



DANE for IPSEC OPPORTUNISTIC ENCRYPTION

IPSECA - IPsec Public Key Discoverable VPN encryption



DANE with OFF-THE-RECORD

OTRFP - OTR Public Keys

Safe key exhange

DANE with BITCOINGS

PMTA - Payment Association

Discoverable secure association between service identifiers and payment information

Why Not DNSSEC

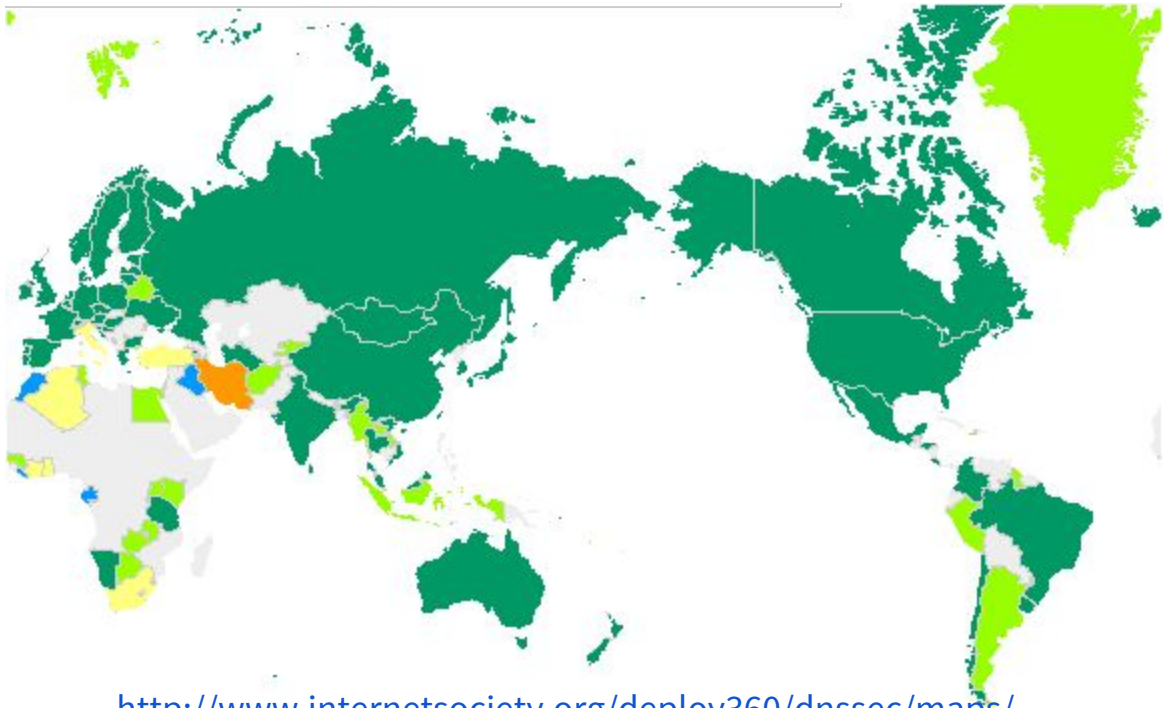
The Arguments Against

1

DNSSEC Requires Critical Mass

Adoption

ccTLD DNSSEC Status 2016-01-04



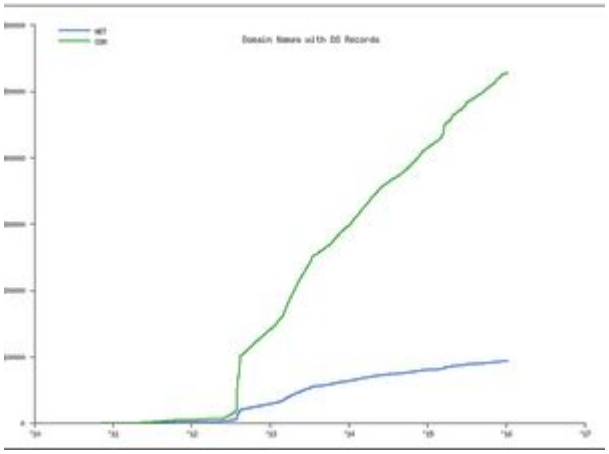
http://www.internetsociety.org/deploy360/dnssec/maps/

- Experimental - Internal experimentation announced or observed
- Announced - Public commitment to deploy
- Partial - Zone is signed but not in operation
- DS in Root - Zone is signed and its DS has been published
- Operational - Accepting signed delegations and DS in root

Second Level Domain Growth

Signed SLDs in .com and .net

http://scoreboard.verisignlabs.com/count-trace.png



Signed SLDs in nTLDs

https://ntldstats.com/dnssec

DNSSEC Validation Usage

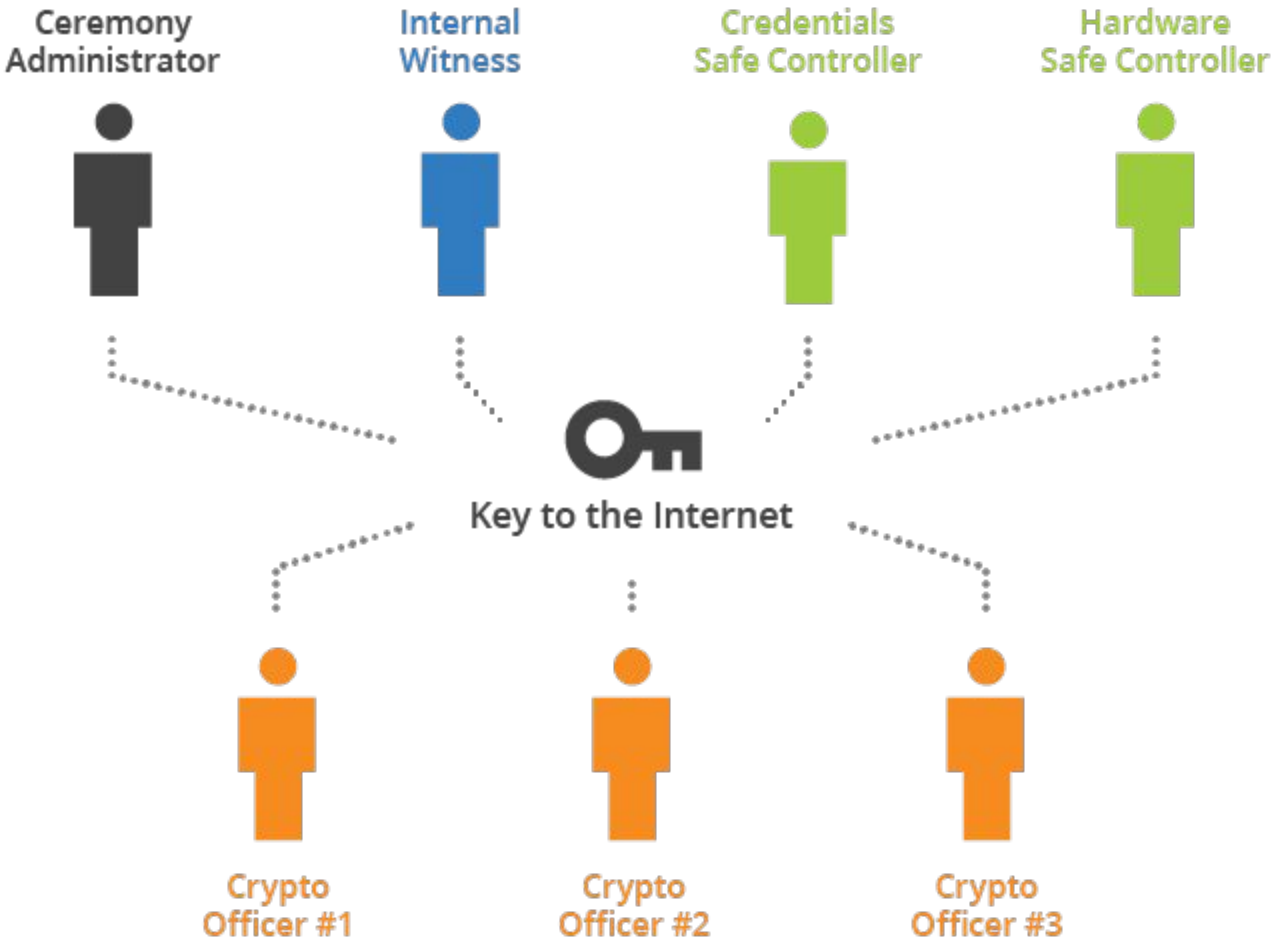
DNSSEC Validates ~25% of queries
in the United States (US)

ADOPTION

- ISPs: Comcast, AT&T, Vodafone, Sprint, Time Warner and many more
- CDNs: CloudFlare, Akamai
- Google Public DNS, Microsoft, Cisco

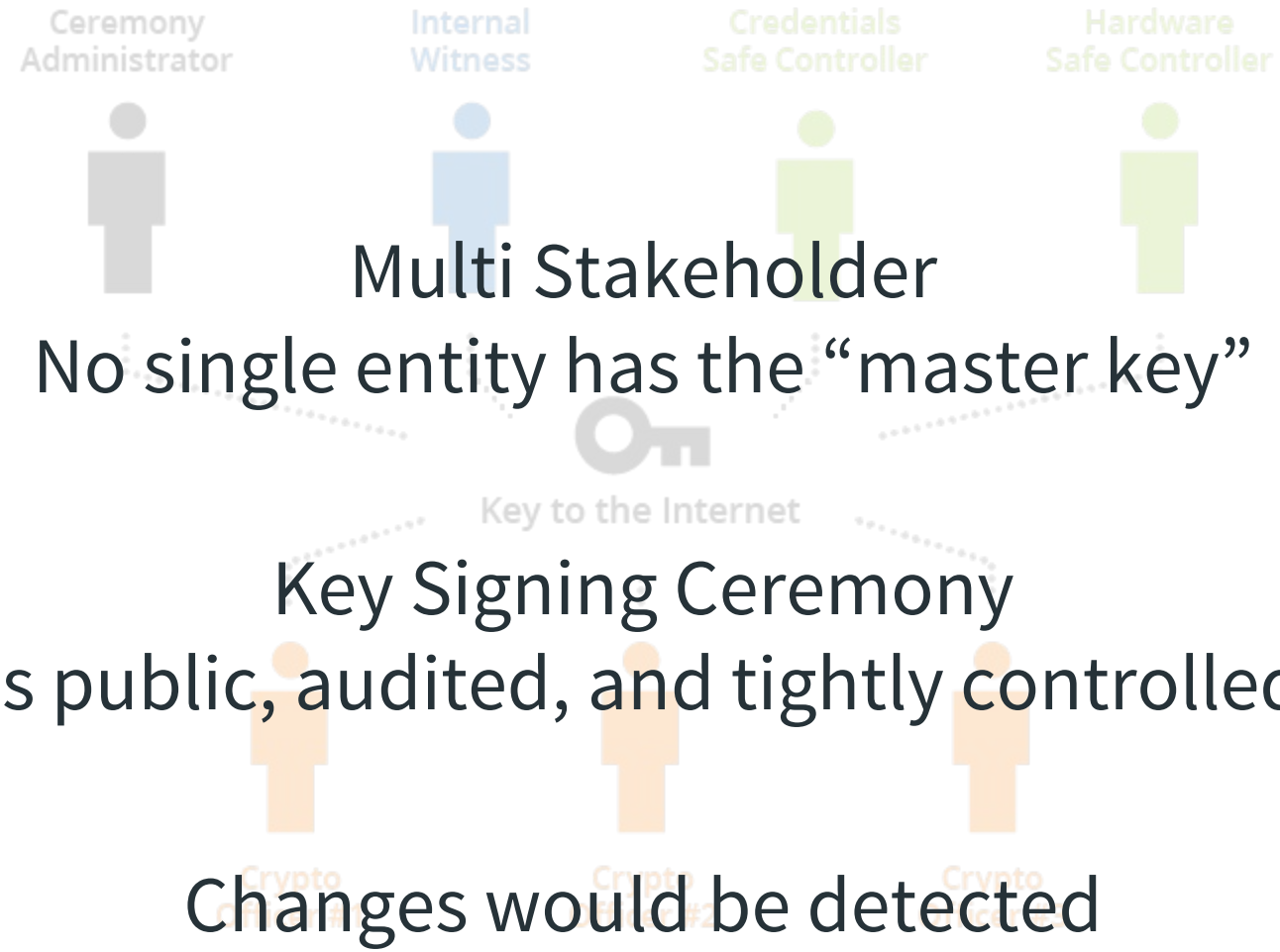
Why Should I Trust Root?

Why Should I Trust Root?



https://www.cloudflare.com/dnssec/root-signing-ceremony/

Why Should I Trust Root?



Multi Stakeholder
No single entity has the “master key”

Key Signing Ceremony
is public, audited, and tightly controlled

Changes would be detected

https://www.cloudflare.com/dnssec/root-signing-ceremony/

1

EXPENSIVE

To Deploy

DNSSEC is EXPENSIVE

- **CPU** - There will be an increase in CPU load. With modern processors most will be okay.
  - Resolvers caching helps
  - Authoritative servers signing frequently or many zones will be more taxed

- **Storage** - Expect zone files to increase at least 3x; storage is inexpensive

DNSSEC is EXPENSIVE

- **RAM** - Larger answer sets and zone files so higher memory usage; 4x as many records; commodity RAM is inexpensive
- **Bandwidth** - 5x larger responses but still relatively small

DNSSEC COMPATIBILITY

Extension Mechanisms for DNS (EDNS0)

- DNS UDP packets larger than 512 bytes
- DNS over TCP

- Non-compliant DNS implementations; Check for fragmentation/truncation
- Adjust ACLs accordingly

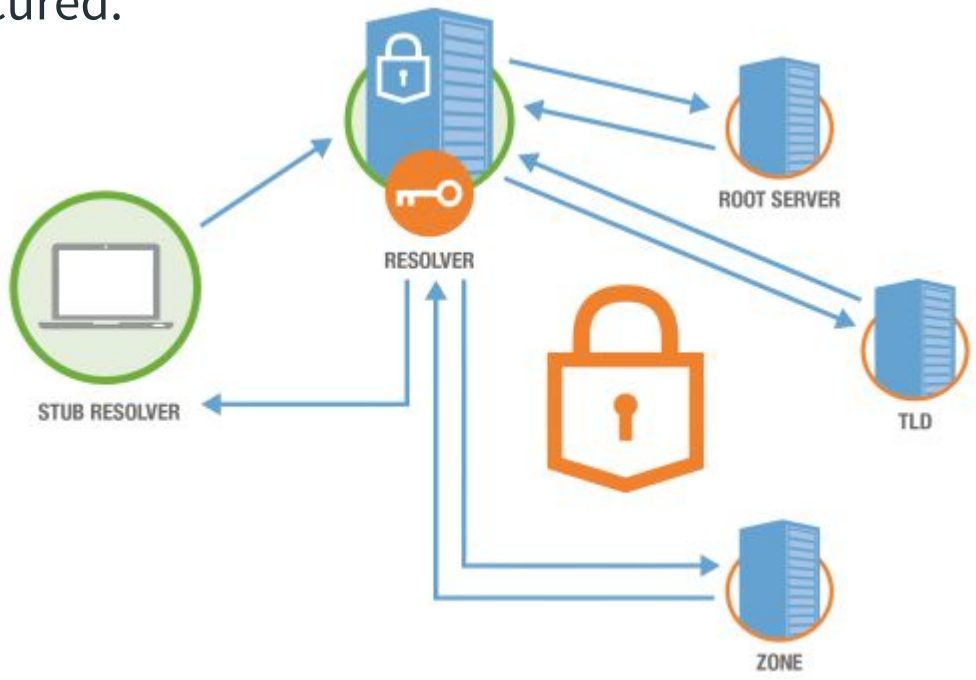
1

Incomplete

“Last Mile” / “First Hop” Issue

“Last Mile” / “First Hop” Issue

- Chain of trust is at the validating resolver, which is traditionally external to the system.
- Communication between the validating DNS server and clients needs to be secured.
- Solutions available, but no standard implementation.



“Last Mile” / “First Hop” Solutions

- getdns: DNSSEC aware applications
  https://getdnsapi.net/
- Fedora’s solutions: Include a validating resolver, Unbound
  https://fedoraproject.org/wiki/Changes/Default_Local_DNS_Resolver
- Microsoft’s solution: IPsec tunnel from every client to the DNS server
  - https://technet.microsoft.com/en-us/library/ee649178%28v=ws.10%29.aspx
- DNScrypt: authenticates communications between a DNS client and resolver
  - https://dnscrypt.org/

1 Alternatives?

ALTERNATIVES

Proposed alternatives:

- Do nothing
- DNSCurve
  Encrypts DNS traffic

ALTERNATIVES

DNSCurve

- Lacking adoption
  Only OpenDNS and Cryptostorm
- Not a question of either/or
  DNSCurve doesn't prevent our adoption of DNSSEC — they are not mutually exclusive.
  - OpenDNS

Take Advantage of DNSSEC

Validation for Desktops

Test If DNSSEC Is Enabled

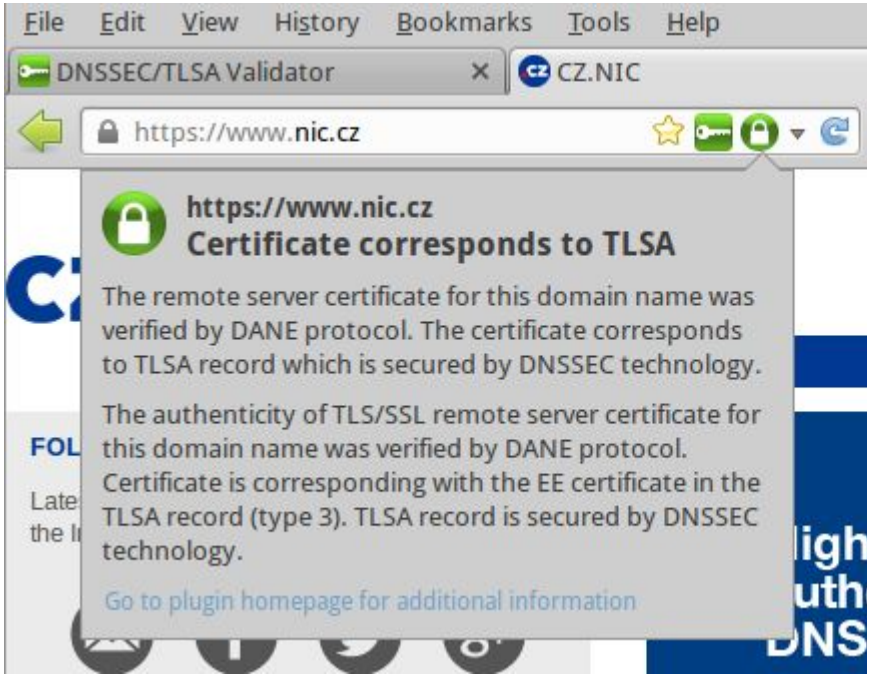
- Is Your Internet Up-to-date?
  http://en.internet.nl/connection/
- SIDN DNSSEC Test
  http://dnssectest.sidn.nl/test.php
- Wildcard domains DNSSEC resolver test
  http://0skar.cz/dns/en/

Use in Browsers

DNSSEC/TLSA Validator

https://www.dnssec-validator.cz

Checks the existence and validity of DNSSEC records and TLSA records

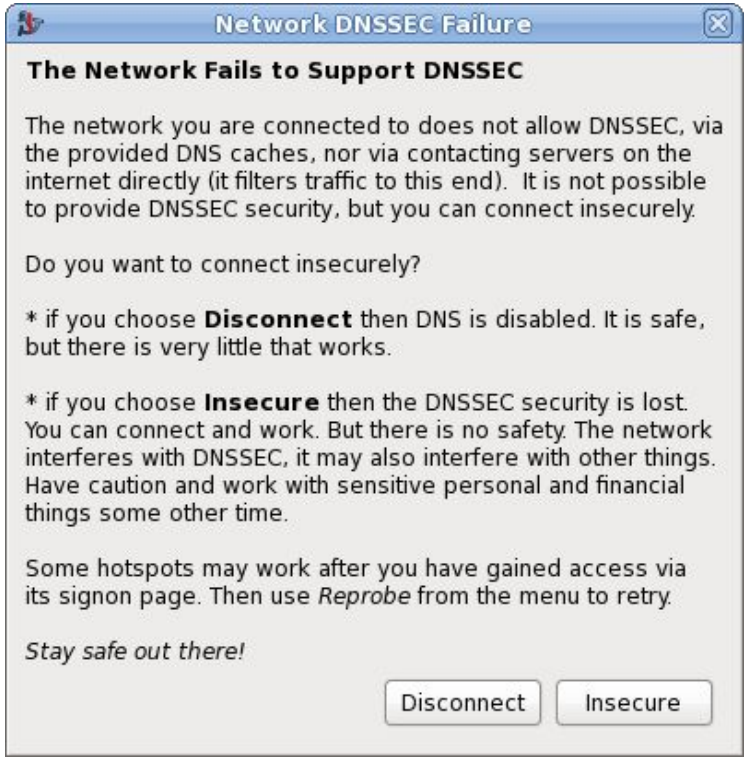


Use a DNSSEC Aware Resolver

DNSSEC-trigger

https://www.nlnetlabs.nl/projects/dnssec-trigger/

Uses Unbound to probe for DNSSEC and configure the resolver accordingly.



Use Open DNSSEC Validating Resolvers

DNS-OARC

https://labs.nic.cz/en/odvr.html

149.20.64.20, 149.20.64.21

2001:4f8:3:2bc:1::64:20, 2001:4f8:3:2bc:1::64:21

CZ.NIC

https://www.dns-oarc.net/oarc/services/odvr

217.31.204.130, 193.29.206.206

2001:1488:800:400::130, 2001:678:1::206

Google Public DNS

https://developers.google.com/speed/public-dns/

8.8.8.8, 8.8.4.4

2001:4860:4860::8888, 2001:4860:4860::8844

Take Advantage of DNSSEC

Validation for Resolvers/Routers

Dnsmasq

Enable DNSSEC Validation

--dnssec \

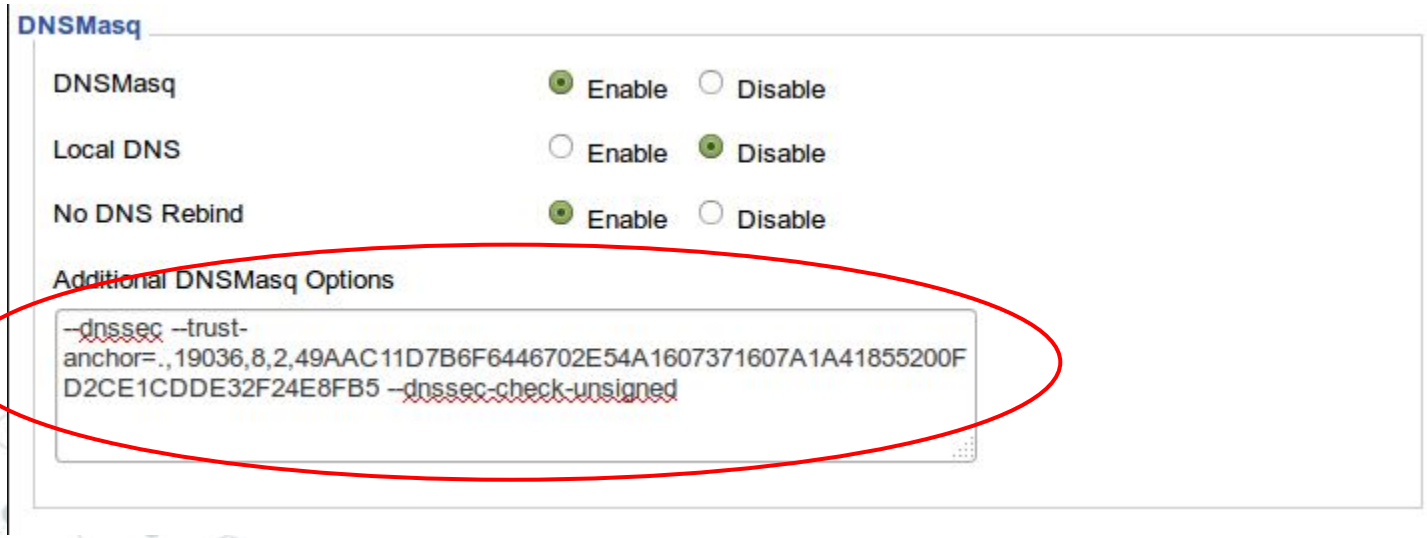
--trust-anchor=.,19036,8,2,49
AAC11D7B6F6446702E54A1607371607A1A418
55200FD2CE1CDDE32F24E8FB5 \

--dnssec-check-unsigned

DD-WRT Enable DNSSEC Validation

Under Services

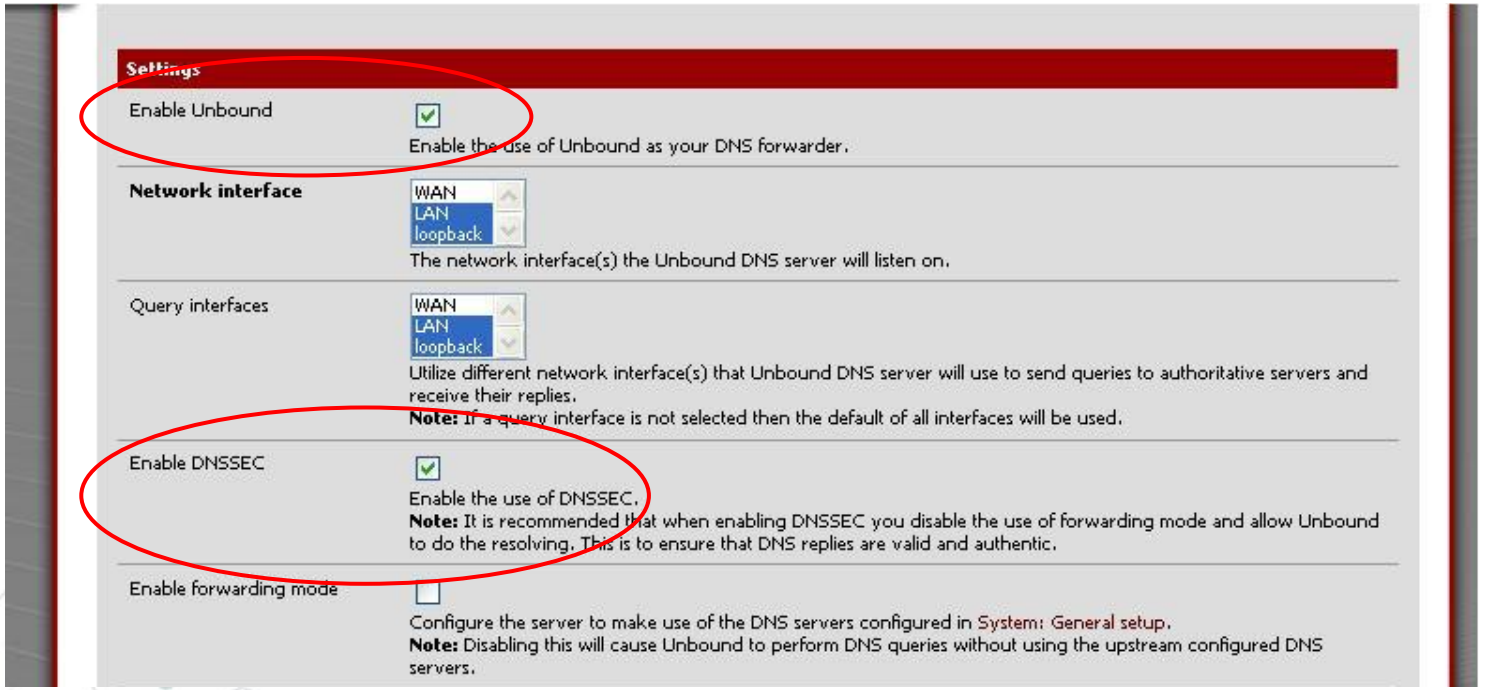
Enter the parameters for Dnsmasq



pfSense Enable DNSSEC Validation

Enabled by default

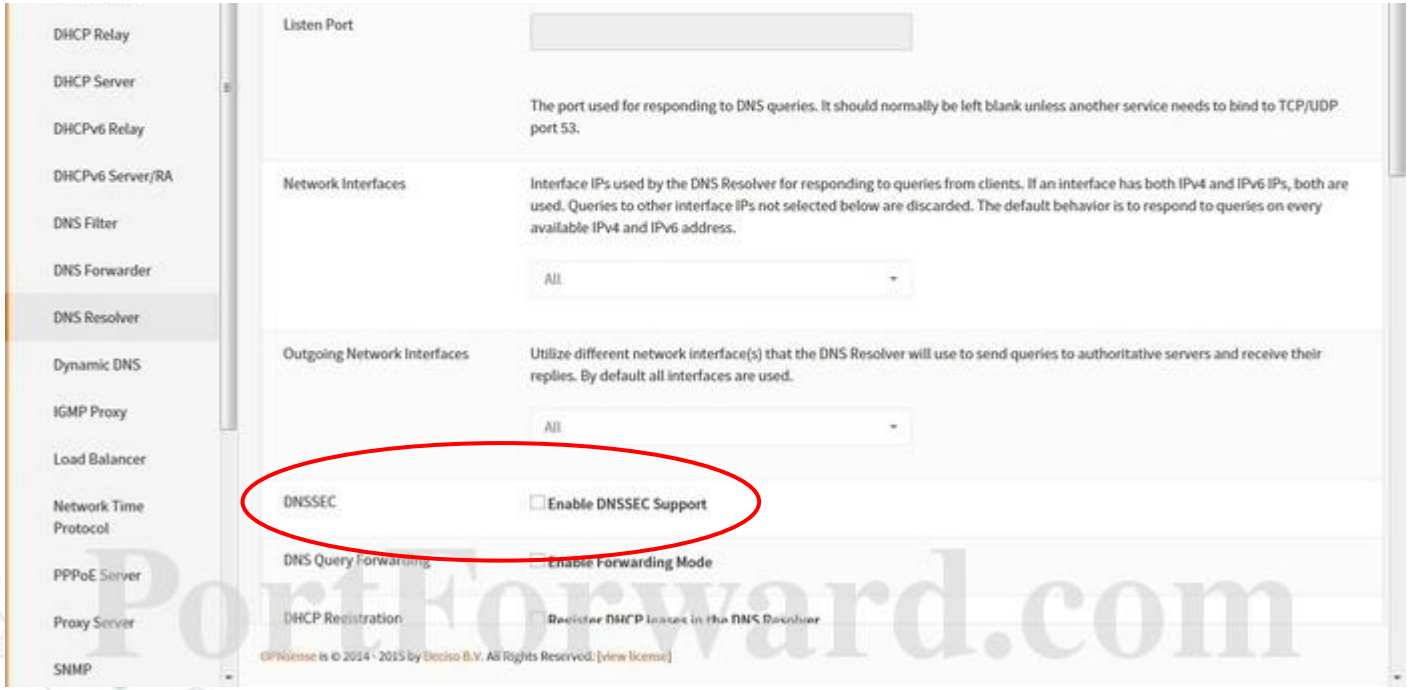
Goto: Services > DNS Resolver



OPNsense Enable DNSSEC Validation

Resolver not enable by default

Goto: Services > DNS Resolver



Take Advantage of DNSSEC

Validation for Applications

Use for UC and VoIP

- Jitsi

  http://www.dnsjava.org/dnsjava-current/Changelog

- Kamailio SIP

  http://www.kamailio.org/w/2013/05/dnssec-support-in-kamailio/

KAMAILIO

Use with Jabber/XMPP

Server

- Prosody
  https://modules.prosody.im/mod_s2s_auth_dane.html
- Tigase (expected in 7.2)
  https://projects.tigase.org/issues/1626

Clients

- Gajim
  http://www.slideshare.net/MenandMice/dane-webinarsep2014
- Irssi
  https://github.com/irssi/irssi/commit/d826896f74925f2e77536d69a3d1a4b86b0cec61

XMPP servers with DANE records

https://xmpp.net/reports.php#dnssecdane

Use Email and TLSA

- Postfix
  Open-source MTA agent that attempts to be fast, easy to administer, and secure.
- Exim
  General and flexible mailer with extensive facilities for checking incoming e-mail.

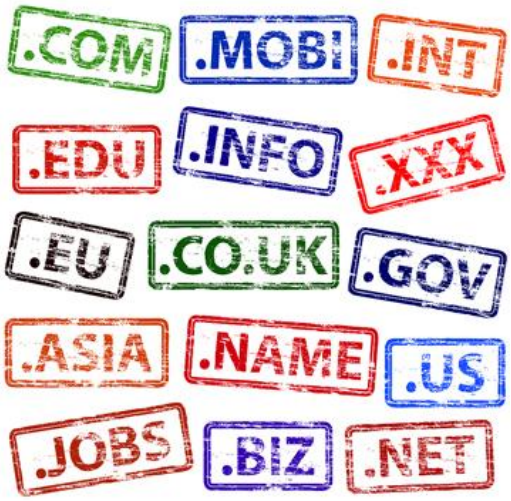
Take Advantage of DNSSEC

Domain Owners and Sysadmins

Using on Domain

Registrars

- Hover
- Gandi
- GoDaddy
- Google



ICANN List:

More: http://www.icann.org/en/news/in-focus/dnssec/deployment

Using Authoritative Servers

- **BIND 9** - DNS reference implementation can automate zone signing, even for dynamic zones.
- **PowerDNS** - Database backend
- **Knot-DNS** - High performance, scales well
- **NSD** - Fast, simple, secure

- **Windows 2012** -Dynamic zone updates with Active Directory; no TLSA until 2016
  https://technet.microsoft.com/en-us/library/dn593674.aspx

Tools

OpenDNSSEC

Open-source turn-key solution for DNSSEC

https://www.opendnssec.org

DNSSEC-Tools

Set of software tools, patches, applications, wrappers, and extensions to ease the deployment of DNSSEC related technologies

http://www.dnssec-tools.org/

Conclusion

It’s almost over

CONCLUDING ACTIONS

- Spread awareness
- Inquire your service provides
- Adopt

Need help?

My contact info is in the slides

Everyone, embrace a safer world

CONCLUSION

- DNS is fundamental to the Internet, but it is unsafe
- DNSSEC is the next evolutionary step in securing the Internet.
- DNSSEC is the foundation for more types of secure data transactions.

Thank You

Carlos Meza

Special thank you to Josh Kuo of the Internet Systems Consortium and DeepDive Networking.

carlos@digitalr00ts.com

@digitalr00ts

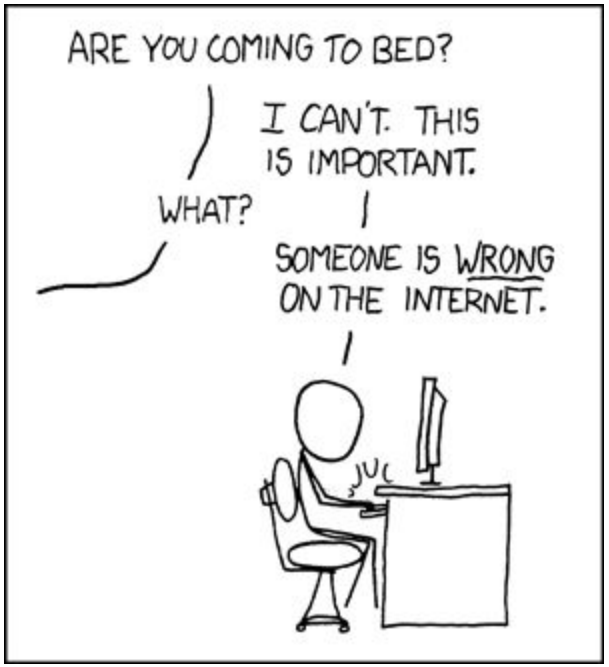
Carlos Meza

carlos@digitalr00ts.com

@digitalr00ts

Troubleshooting

When Duty Calls



https://xkcd.com/386/

Common Problems

Security Lameness

Similar to Lame Delegation but with DS RRs instead of NS RRs, resulting in a broken chain-of-trust.

Incorrect Time

Keys and certificates that have a validity time frame are dependant on correct time.

Invalid Trust Anchors

Will cause all queries to fail

http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html#troubleshooting-common-problems

DNS Lookup Utilities

Option	dig	drill
Set DO bit	+dnssec	-D
Trace delegation	+trace	-T
Chase signatures	+sigchase	-S
Set CD bit	+[no]cdflag	-o CD / -o cd
Return equivalent DS for DNSKEY		-s
Use TCP	+tcp	-t

Web Hosted Tools

- Hostmaster
  https://www.zonemaster.net
- DNSSEC Debugger
  http://dnssec-debugger.verisignlabs.com/
- Keytool
  http://keytool.verisignlabs.com/
- DNSViz
  http://dnsviz.net/

DNSSEC Test Sites

Valid Delegation and DANE

- OpenDNSSEC
  https://www.opendnssec.org/
- Fedora
  https://getfedora.org/
- DANE Test Pages
  http://dane.verisignlabs.com/

Intentionally Broken Delegations

- dnssec.fail
  http://dnssec.fail
- Broken DNSSEC Validation Test Site
  http://www.dnssec-failed.org/
- CZ.NIC
  http://www.rhybar.cz/setlang/?language=en

For More Information

Further Reading and My Sources

Resources - Learning more

- Men & Mice - DNSSEC best practices
  https://www.menandmice.com/resources/educational-resources/webinars/dnssec-best-practices-webinar/
- ISC BIND DNSSEC Guide
  http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html
- SIDN DNSSEC Course
  http://www.dnsseccursus.nl/
- Mike Lucas - DNSSEC in 50 Minutes
  part 1 - https://www.youtube.com/watch?v=lY6HgZmAfqc
  part 2 - https://www.youtube.com/watch?v=Hm93GhenqXo
- RIPE NCC - DNSSEC Training Slides
  https://www.ripe.net/support/training/material/dnssec-training-course/DNSSEC-Slides-Single.pdf
- Internet Society
  http://www.internetsociety.org/deploy360/dnssec/

Resources - Learning Even More

- An Illustrated Guide to the Kaminsky DNS Vulnerability
  http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
- Verisign Labs with DANE http://www.verisign.com/en_US/innovation/verisign-labs/dane-protocol/index.xhtml

References

- Domain Name System (DNS) Parameters
  http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml
- DNS Glossary
  http://www.menandmice.com/support-training/support-center/knowledgehub/dns-glossary/
- DNSSEC RFCs
  https://www.icann.org/resources/pages/standards-2012-02-25-en

Thank You

Carlos Meza

Special thank you to Josh Kuo of the Internet Systems Consortium and DeepDive Networking.

carlos@digitalr00ts.com

@digitalr00ts

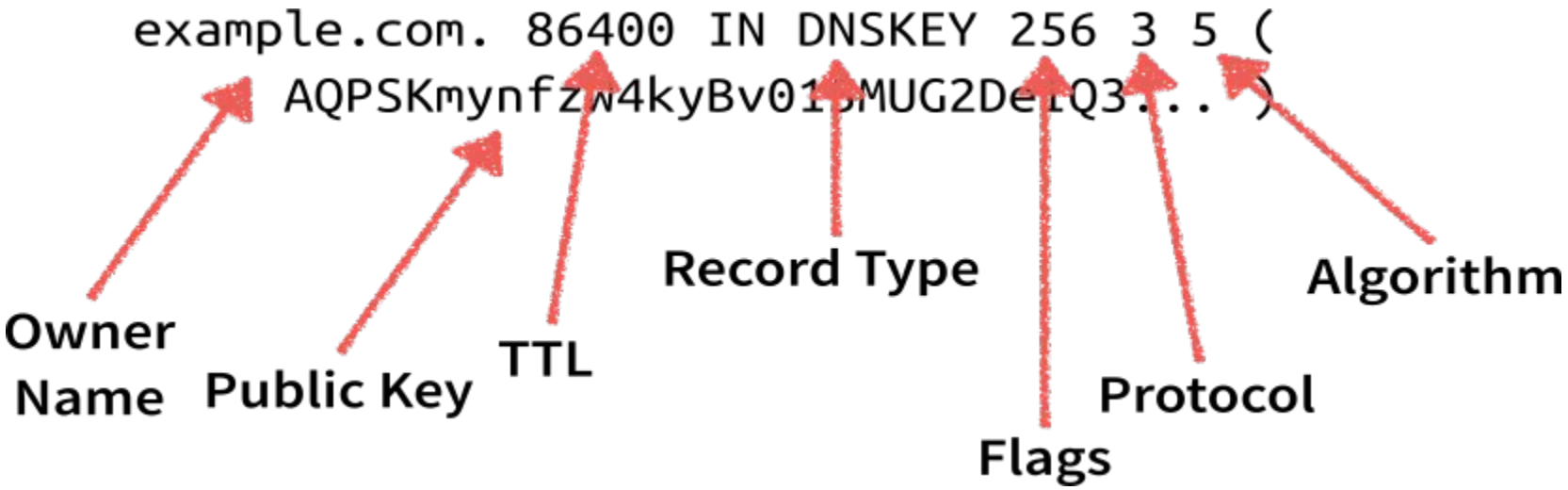
Technically Speaking

Records, Algorithms, Key Rollovers

DNSSEC Bits

- **DO - DNSSEC OK**
  Indicates the resolver is requesting and able to accept DNSSEC
- **CD - Checking Disabled**
  Indicates the resolver is intentionally does not want validation, even if available
- **AD - Authenticated Data**
  Indicates in a response that the data has been verified

DNSKEY RR

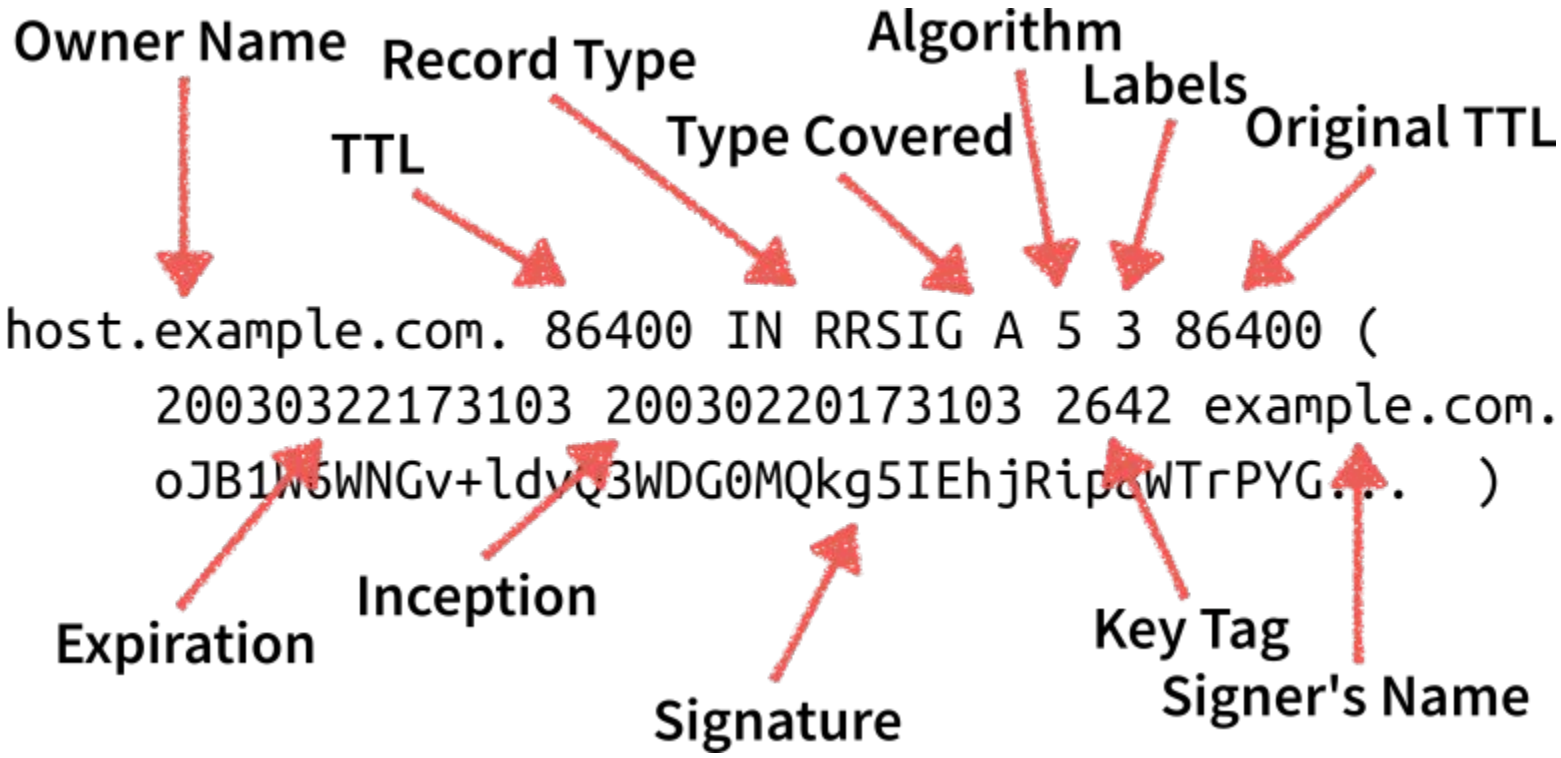


Flags : 256 - Zone Signing Key, 257 - Key Signing Key

Protocol fixed value 3; for backward compatibility with early versions of the KEY record

http://tools.ietf.org/html/rfc4034#section-2

RRSIG RR



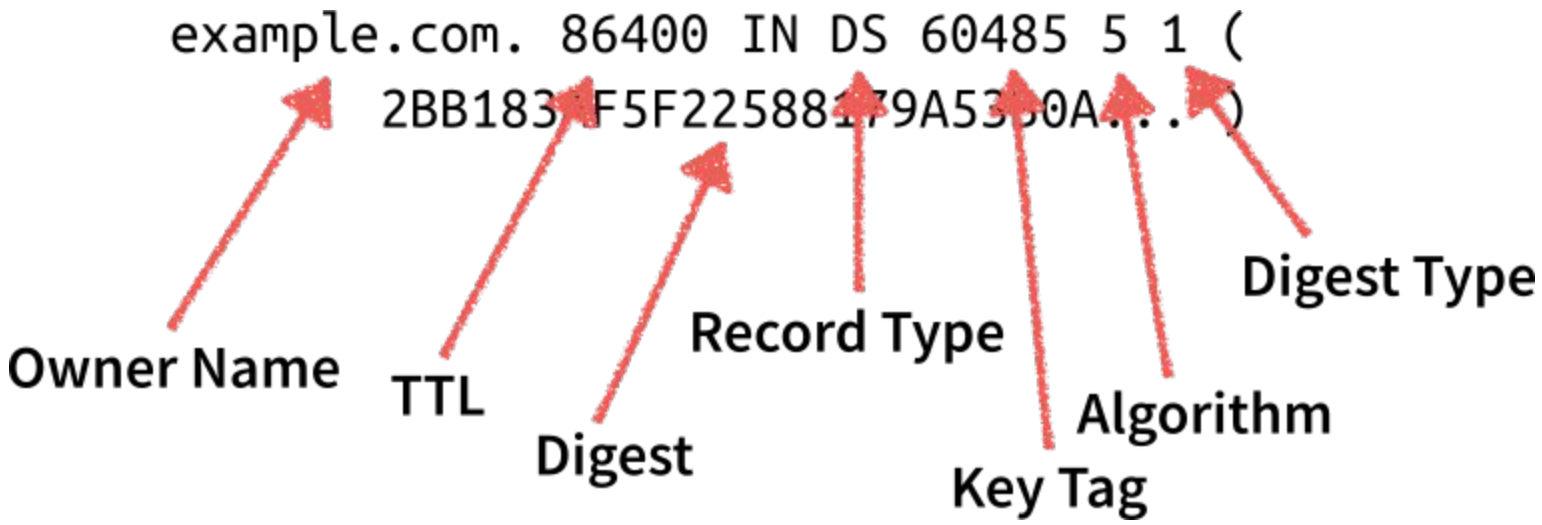
Signature = sign(RRSIG_RDATA + RR(1) + RR(2)...)

RRSIG_RDATA is the RRSIG RDATA fields with the Signer's Name field in canonical form and the Signature field excluded

RR(i) = owner + type + class + TTL + RDATA length + RDATA

http://tools.ietf.org/html/rfc4034#section-3

DS RR



Digest = digest_algorithm(DNSKEY owner name + DNSKEY RDATA)

DNSKEY RDATA = Flags + Protocol + Algorithm + Public Key

Digest Type: Hash algorithm used to create the Digest value
1 - SHA-1 | 2 - SHA-256 | 3 - GOST R 34.11-94 | 4 - SHA-384

http://tools.ietf.org/html/rfc4034#section-5

DNSSEC Resource Records

- NSEC/NSEC3/NSEC5 - Denial of existence
  - NSEC3PARAM - Hash type, iterations, salt, etc

TLSA Certificate Association

With current CA system

1 - “CA constraint”
Specifies which CA to use
2 - “Service certificate constraint”
Specifies which certificate is valid

Without current CA system

3 - “trust anchor assertion”
Domain has its own CA
4 - “domain-issued certificate”
Certificate w/o need of third party

http://tools.ietf.org/html/rfc6698

Algorithms

1 - RSA/MD5 [RSAMD5]

2 - Diffie-Hellman [DH]

3 - DSA/SHA1 [DSA]

4 - Elliptic Curve [ECC]

5 - RSA/SHA-1 [RSASHA1]

6 - DSA-NSEC3-SHA1 [DSA-NSEC3-SHA1]

7 - RSASHA1-NSEC3-SHA1 [RSASHA1-NSEC3-SHA1]

8 - RSA/SHA-256 [RSASHA256]

http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml

9 - Reserved

10 - RSA/SHA-512 [RSASHA512]

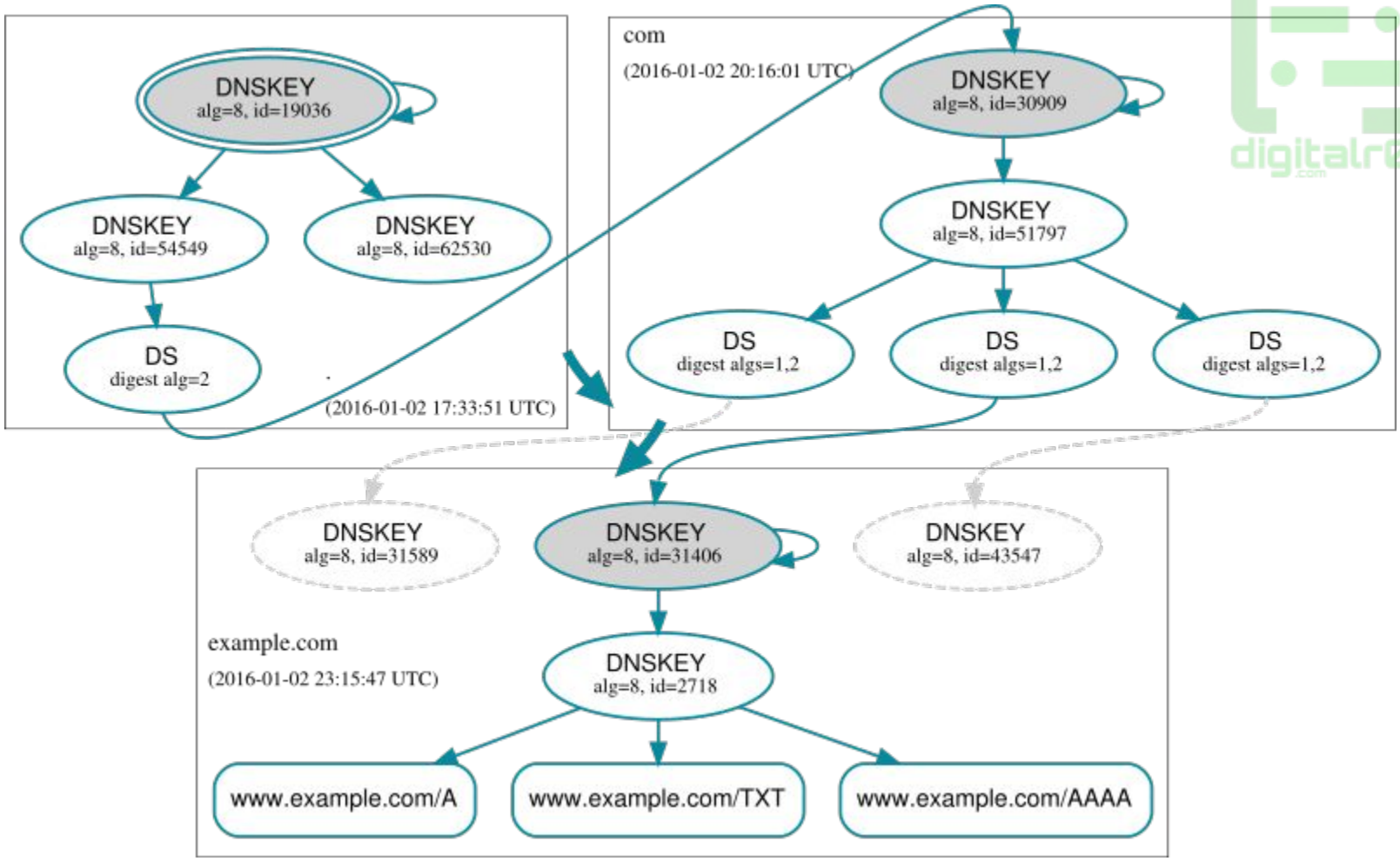
11 - Reserved

12 - GOST R 34.10-2001 [ECC-GOST]

13 - ECDSA Curve P-256 with SHA-256 [ECDSAP256SHA256]

14 - ECDSA Curve P-384 with SHA-384

[ECDSAP384SHA384]



Chain of Trust - example.com

Changing Keys

The ZSK publishes more signatures than the KSK, giving attackers more data to work with.

- ZSK - Change every 3 to 12 months
- KSK - Change every years 2 - 5 years; Use stronger encryption than ZSK

Extra signatures and keys are okay as long as as there is a validate a chain of trust.

Rollover Methods - ZSK

Pre-publication

Smaller zone file, but more steps

1. Publish new ZSK
2. Generate new RRSIG after at least one TTL
3. Removing the old key after at least another TTL

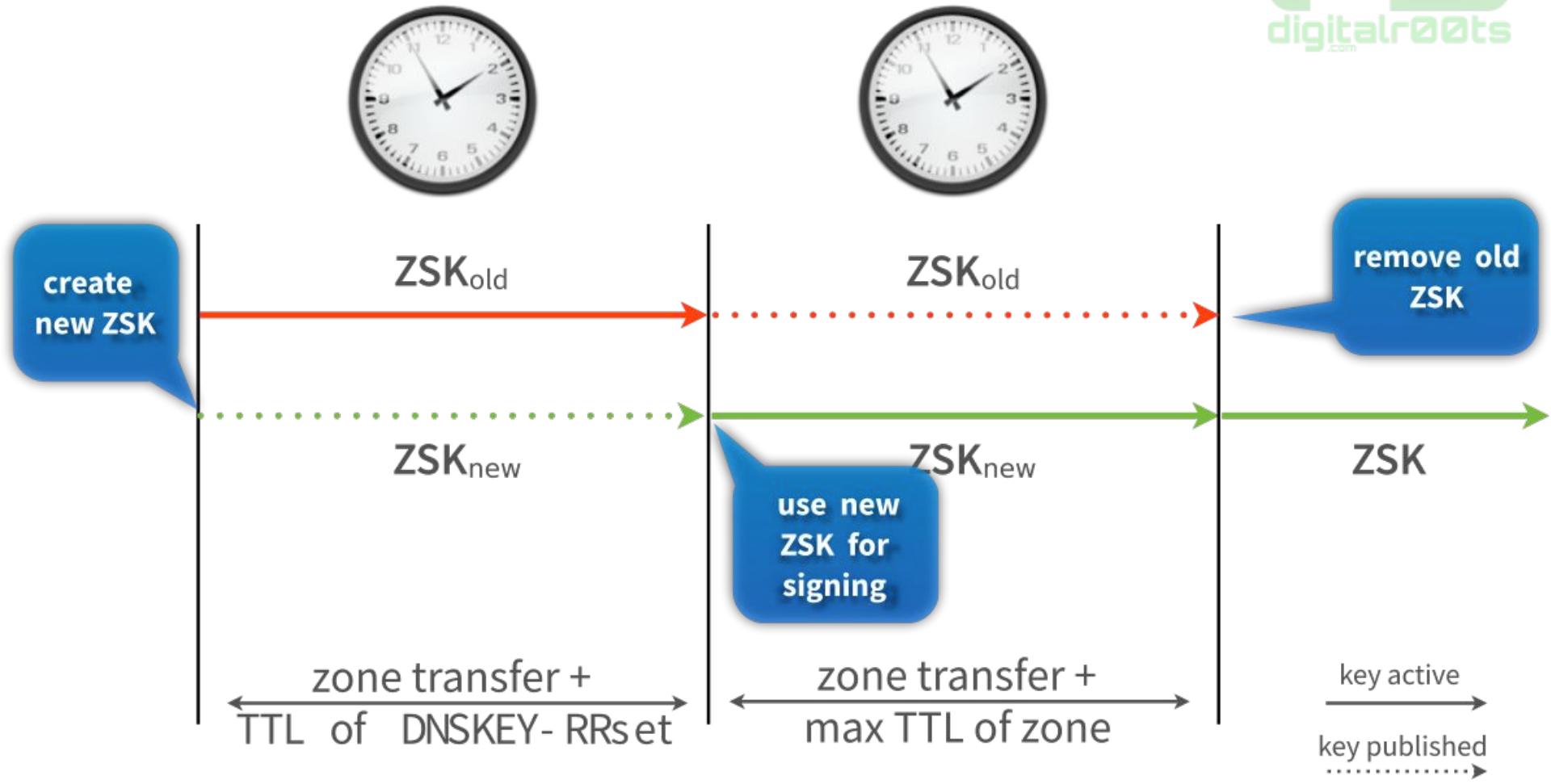
Double Signature

Simpler but larger zone files

1. Publish new ZSK and sign zone
2. Remove old ZSK and RRSIGs after at least one TTL

http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html#key-rollovers

ZSK Pre-publication Rollover



https://www.menandmice.com/resources/educational-resources/webinars/dnssec-best-practices-webinar/

Rollover Methods - KSK

Double-DS

DNSKEY RRset is smaller, but 2 updates to parent zone

1. Publish new DS record
2. Change key after longest TTL
3. Remove old DS record after longest TTL

Double-KSK

Single update to parent zone, but larger DNSKEY RRset

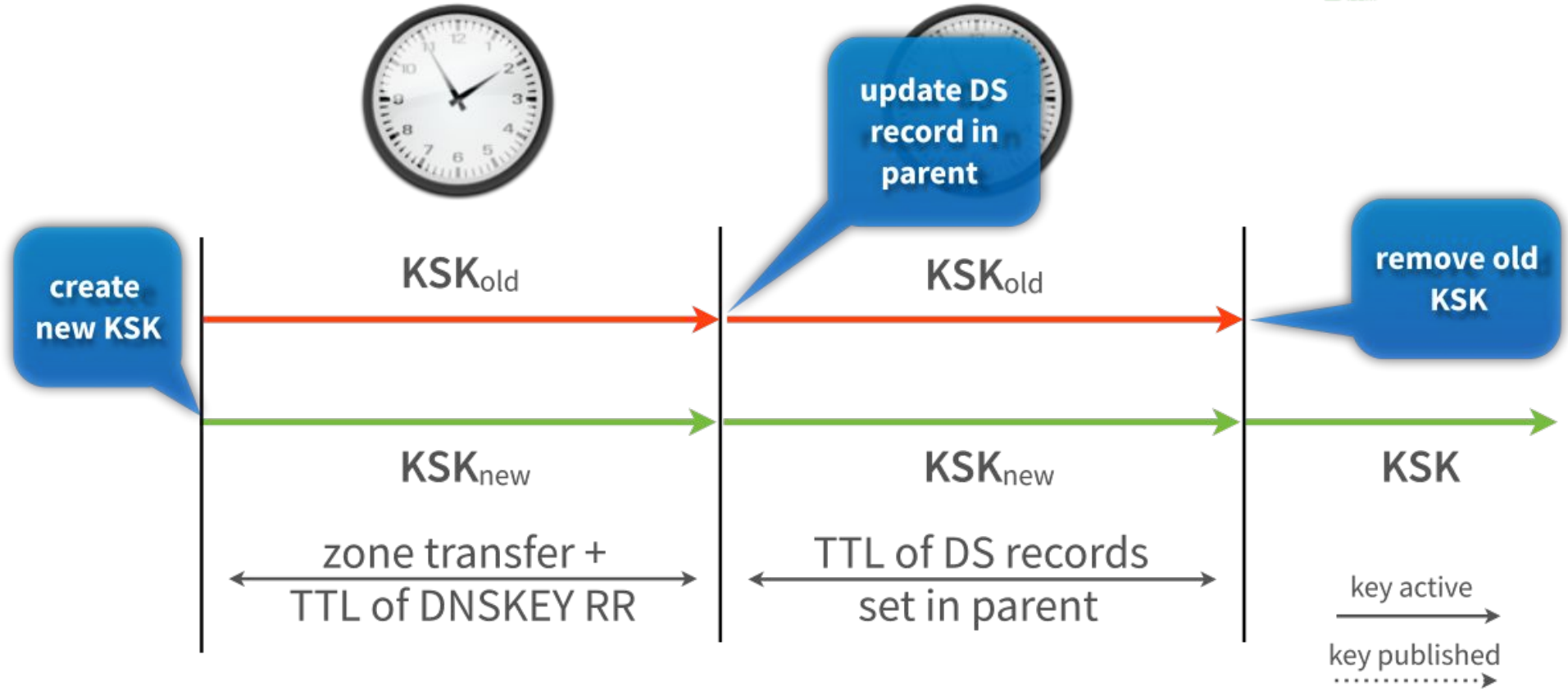
1. New DNSKEY RRset;
   2 KSK + RRSIGs
2. Update DS record after longest TTL
3. Remove old key after longest TTL

Double-RRset

Fastest, but larger DNSKEY RRset and 2 updates to parent zone

1. Publish new DS RR and DNSKEY RRset
2. Remove old DS RR and key after longest TTL

KSK Double-Key Rollover



https://www.menandmice.com/resources/educational-resources/webinars/dnssec-best-practices-webinar/

Using Hosted DNS (Free)

- RollerNet Secondary Server
  https://acc.rollernet.us/help/dns/secondary.php
- PUCK Free Secondary DNS Service
  https://puck.nether.net/dns/
- GratisDNS (in Danish)
  https://gratisdns.dk
- 1984Hosting
  https://www.1984hosting.com/product/freedns/
- DNS4.PRO
  https://dns4.pro

- Hurricane Electric is evaluating DNSSEC
  https://dns.he.net/

Thank You

Carlos Meza

Special thank you to Josh Kuo of the Internet Systems Consortium and DeepDive Networking.

carlos@digitalr00ts.com

@digitalr00ts

Using DANE

Use with Hosted Email

- Posteo
  https://posteo.de/blog/posteo-unterst%C3%BCtzt-danetlsa
- mailbox.org
  https://mailbox.org/dane-und-dnssec-fuer-sicheren-e-mail-versand-bei-mailbox-org/
- Dotplex
  https://secure.dotplex.de/webhosting/secure-hosting
- mail.de
  https://mail.de/unternehmen/presse/2014-06-19-mailde-unterstuetzt-dane-tls
- Tutanota.de
  https://tutanota.com/blog/posts/dane-everywhere

Use Web-based Tools

- DANE SMTP Validator
  https://www.tlsa.info
- DANE/TLS Testing
  https://www.had-pilot.com/dane/danelaw.html
- Generate TLSA Record
  https://www.huque.com/bin/gen_tlsa
- OPENPGPKEY RR Generator
  https://www.huque.com/bin/openpgpkey

  Calculate SMIMEA Record
  https://www.co.tt/smimea.cgi
- DANE SMIMEA Toolset (tests for support)
  http://dst.grierforensics.com

Examples

compare signed and unsigned zone file

DNSSEC Key Sizes

(packet size and computation considerations)

https://www.youtube.com/watch?v=ZHdcFJQOEto @ 20min

Tools

Web Hosted Tools

Validate

http://en.internet.nl/connection/

http://www.verisign.com/en_US/innovation/verisign-labs/internet-security-tools/index.xhtml

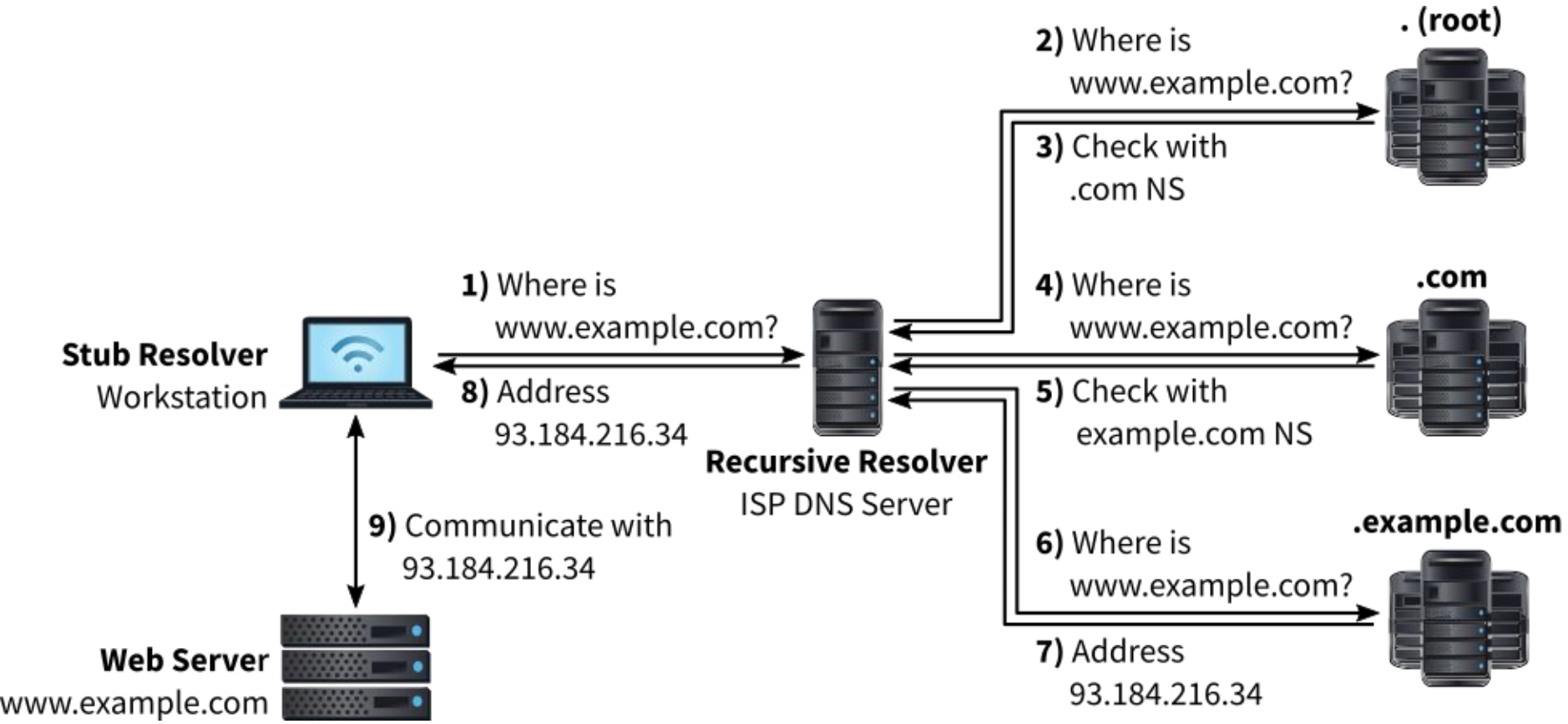
https://www.dns-oarc.net/oarc/services/replysizetest

Statistics

http://stats.sidnlabs.nl/#dnssec

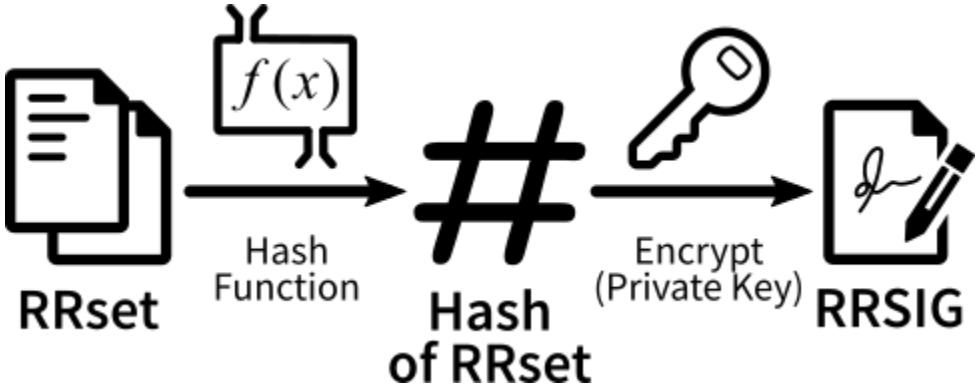
DNSSEC - Validation

DNS Lookup

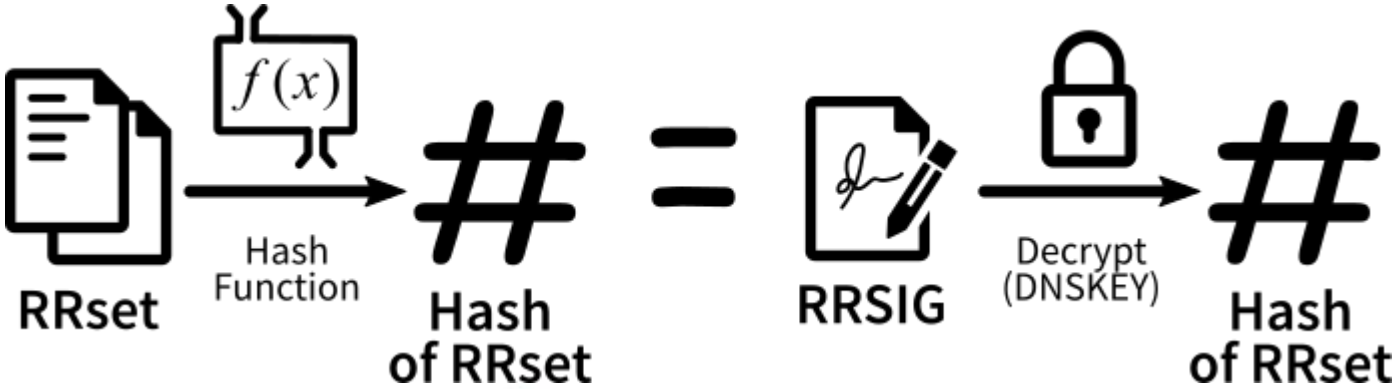

. (root)
2) Where is www.example.com?
3) Check with .com NS
.com
4) Where is www.example.com?
5) Check with example.com NS
.example.com
6) Where is www.example.com?
7) Address 93.184.216.34
Authoritative Nameservers
1) Where is www.example.com?
8) Address 93.184.216.34
Stub Resolver
Workstation
Recursive Resolver
ISP DNS Server
9) Communicate with 93.184.216.34
Web Server
www.example.com

Signing and Verification

Sign (Authoritative Nameserver)



Validate (Validating Recursive Resolver)



Adoption - TLDs

- 2005 - .se (Sweden) is the first TLD signed
- 2007 - .pr (Puerto Rico), .br (Brazil), .bg (Bulgaria)
- 2008 - .cz (Czech Republic) signed
- 2008 - .gov mandate to sign all domains
- 2009 - .org is the first signed gTLD
- **2010 July 15, at 2050 UTC - Root signed**
- 2010 - .edu, .net
- 2011 - .com

Adoption

- 2012 - FCC recommends DNSSEC; AT&T, CenturyLink, Cox, Verizon, Sprint, Time Warner pledge to comply
  http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf
- 2013 - Google Public DNS enables DNSSEC validation
  https://googleonlinesecurity.blogspot.com/2013/03/google-public-dns-now-supports-dnssec.html
- 2014 - Dnsmasq 2.69 can validate DNSSEC
  http://lists.thekelleys.org.uk/pipermail/dnsmasq-discuss/2014q2/008416.html
- 2015 - CloudFlare launches Universal DNSSEC
  https://blog.cloudflare.com/introducing-universal-dnssec/

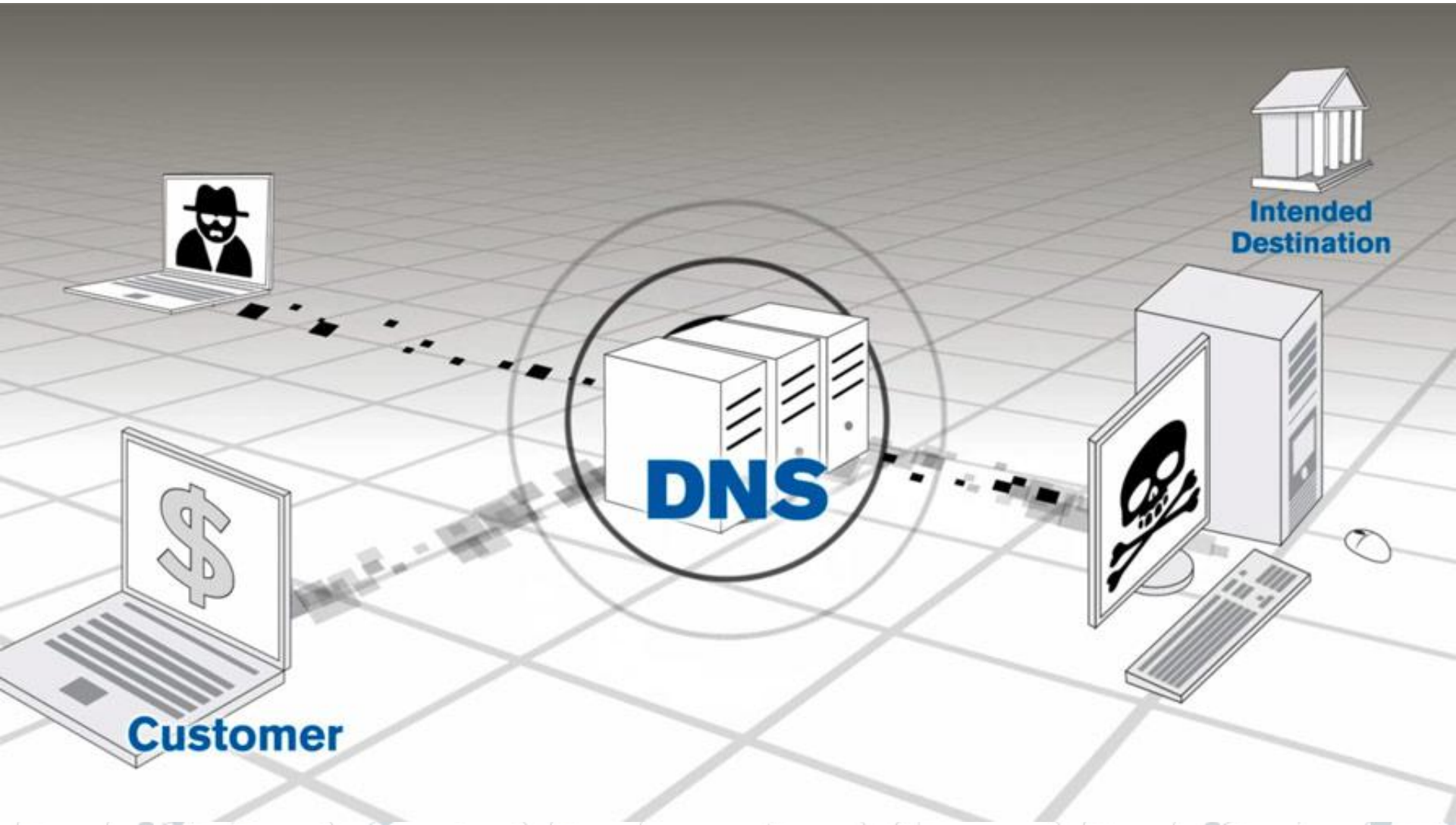
Adoption - TLDs

- 2012 - New gTLDs must be signed
  https://archive.icann.org/en/topics/new-gtlds/draft-rfp-clean-04oct09-en.pdf
- 2012 - .nl signed and becomes first TLD to supasses 1,000,000 signed domains
  http://www.internetsociety.org/deploy360/blog/2012/09/nl-becomes-first-tld-to-pass-1-million-dnssec-signed-domain-names/
- 2013 - ICANN requires registrars to support DNSSEC
  http://www.internetsociety.org/deploy360/blog/2013/09/icanns-2013-raa-requires-domain-name-registrars-to-support-dnssec-ipv6/

Adoption

- 2000 - Verisign DNSSEC contributor
  http://www.verisign.com/en_US/innovation/dnssec/dnssec-test/index.xhtml
- 2010 - GoDaddy, Dyndns.com and NamesBeyond Support DNSSEC
  https://pir.org/go-daddy-dyndns-com-and-namesbeyond-support-dnssec-signed-org-domain-names/
- 2010 - Akamai adds DNSSEC support
  https://www.akamai.com/us/en/about/news/press/2010-press/akamai-adds-support-for-dnssec-to-its-enhanced-dns-service.jsp
- 2012 - Comcast, largest and 1st ISP, completes DNSSEC deployment
  http://corporate.comcast.com/comcast-voices/comcast-completes-dnssec-deployment

DNS was not designed to be secure



DNS Exploits

- 2007 - 2011 - DNSChanger/RSPlug
  http://krebsonsecurity.com/2011/11/malware-click-fraud-kingpins-arrested-in-estonia/
- 2009 - Twitter has DNS Hijacked by “Iranian cyber army” (Baidu was next)
  http://gizmodo.com/5429365/twitter-hacked-hijacked-by-the-iranian-cyber-army-updated
- 2010 - China ISP DNS cache poisoning for Gmail phishing
  https://advox.globalvoices.org/2010/08/11/china-isp-level-gmail-phishing/
- 2010 - Tunisia Gmail phishing though DNS cache poisoning
  https://advox.globalvoices.org/2010/07/05/mass-gmail-phishing-in-tunisia/

DNS Exploits

- 2010 - China's Poisoned DNS cache gets replicated worldwide
  http://www.computerworld.com/article/2516831/security0/china-s-great-firewall-spreads-overseas.html
- 2010 - Google public DNS redirect to Romania and Austria
  http://www.bgpmon.net/googles-services-redirected-to-romania-and-austria/
- 2011 - Brazilian ISPs fall victim DNS cache poisoning
  https://securelist.com/blog/incidents/31628/massive-dns-poisoning-attacks-in-brazil-31/
- 2013 - Win32/Sality gains ability to change a residential router's DNS
  http://www.welivesecurity.com/2014/04/02/win32sality-newest-component-a-routers-primary-dns-changer-named-win32rbrute/

DNS Exploits

- 2014 - Turkey intercepts Google's public DNS service https://googleonlinesecurity.blogspot.com/2014/03/googles-public-dns-intercepted-in-turkey.html
- 2014 - BGP misconfiguration routes Google public DNS to Venezuela
  http://arstechnica.com/information-technology/2014/03/google-dns-briefly-hijacked-to-venezuela/
- 2015 - Malaysia Airlines website DNS hijacked by Lizard Squad
  http://www.bbc.com/news/world-asia-30978299
- 2015 - Google.com.vn and Lenovo.com victim of DNS attack
  http://www.pcworld.com/article/2889392/like-google-in-vietnam-lenovo-tripped-up-by-a-dns-attack.html

SSL/TLS Can't Save You

SSL/TLS provides privacy and data integrity between two applications.

SSL/TLS, What is it?

SSL (Secure Sockets Layer) establishes an encrypted connection between a web server and a browser.

All data passed over this connection is secure.

TLS (Transport Layer Security) is the successor to SSL, but is often referred to as SSL as well.

SSL/TLS Certificate Authorities

SSL/TLS uses certificates obtained from a 3rd party called a CA (Certificate Authority).

SSL/TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate.

SSL/TLS Vulnerability

BEAST

Cipher block chaining (CBC) vulnerability

Heartbleed

Vulnerability in the OpenSSL allowing memory to be read

POODLE

Downgrade attack causing clients to fallback to SSLv3

FREAK

Forces cryptographic downgrade

SSL/TLS Vulnerability

BEAST

Cipher block chaining (CBC) vulnerability

Heartbleed

Vulnerability in the OpenSSL allowing memory to be read

HTTPS Bicycle Attack

POODLE

Downgrade attack causing clients to fallback to SSLv3

FREAK

Forces cryptographic downgrade

Known Attacks on Transport Layer Security RFC 7457

SSL Stripping

STARTTLS

BEAST

Padding Oracle Attacks

Attacks on RC4

CRIME, TIME, & BREACH

RSA-Related Attacks

Theft of RSA Private Keys

Diffie-Hellman Parameters

Renegotiation

Triple Handshake

Virtual Host Confusion

Denial of Service

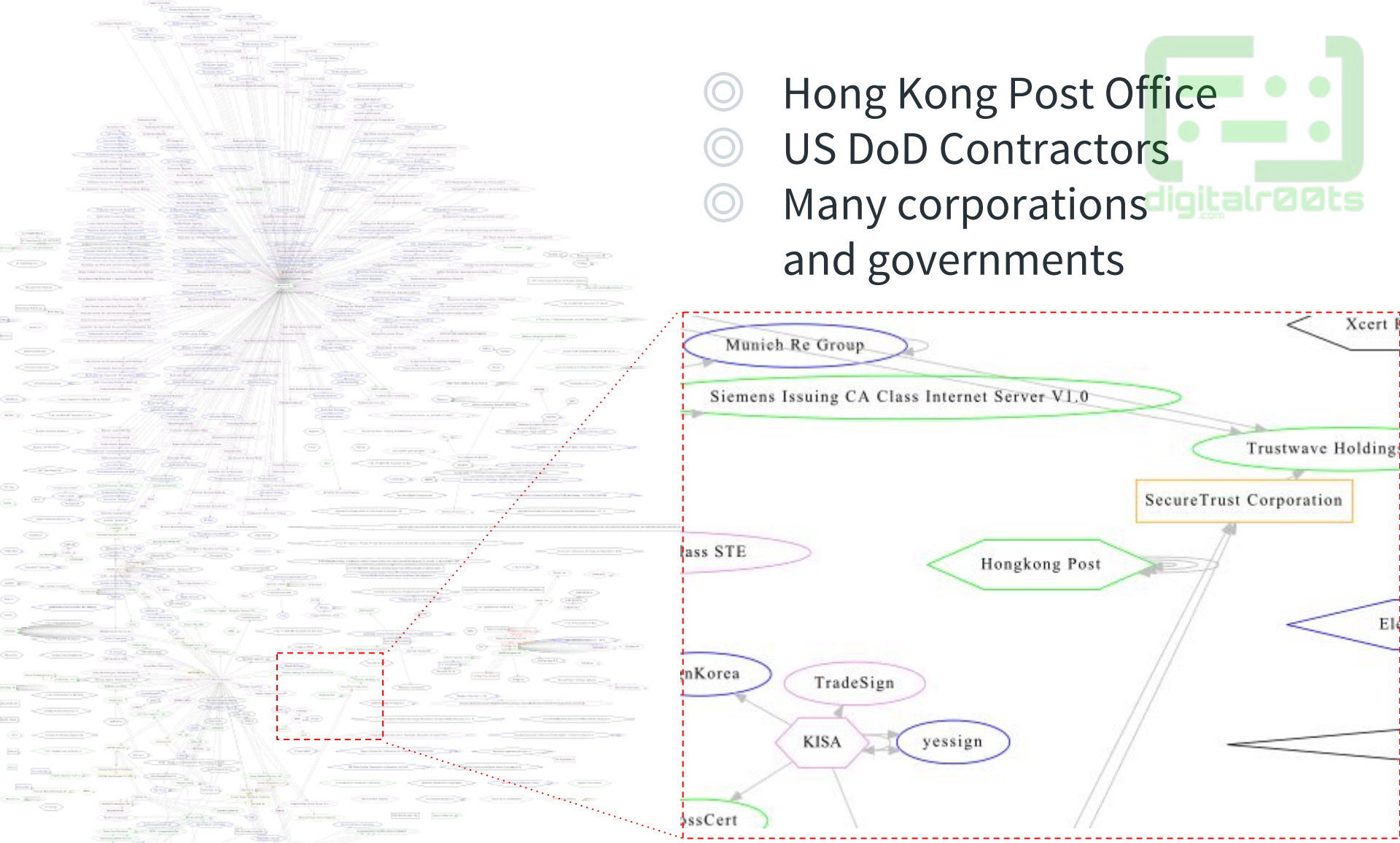
Implementation Issues

Usability

RFC Predates Logjam, FREAK, Bicycle

https://tools.ietf.org/html/rfc7457

- Hong Kong Post Office
- US DoD Contractors
- Many corporations and governments



Too Many CAs

https://www.eff.org/observatory

General CA Issues

- Any CA can issue certificates for any entity on the Internet
- CAs delegate trust to subordinate certification authorities
- CA-signed certificates for unqualified domain names, i.e. localhost, exchange, webmail
  https://www.eff.org/deeplinks/2011/04/unqualified-names-ssl-observatory
- Trust of a CA requires storage of a CA's root certificate in the client's certificate store. This can be tampered

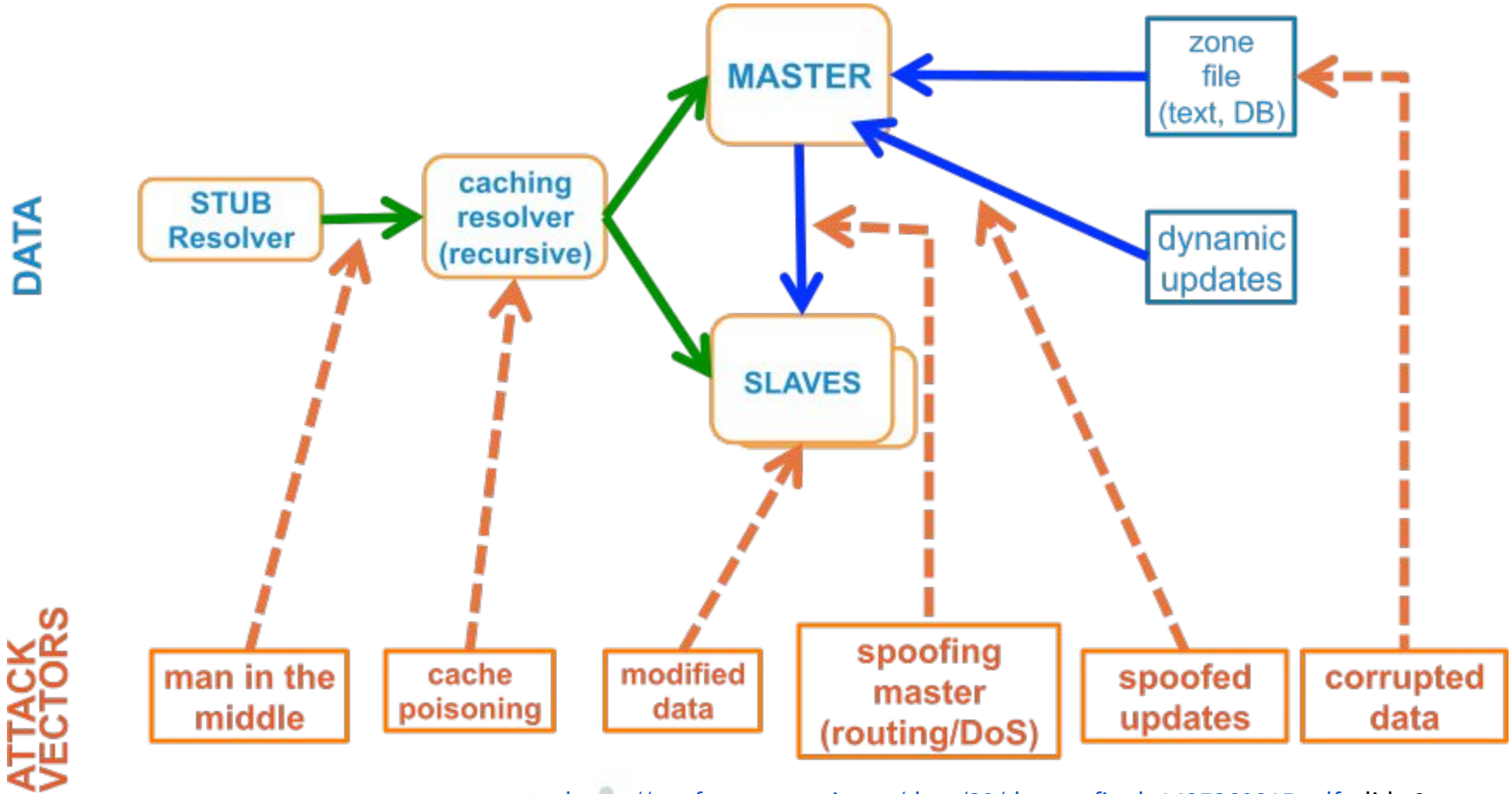
CAs are vulnerable

- 2011 - Comodo breach results in fraudulent certificates being issued
  https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html
- 2011 - DigiNotar compromise results in issuing of fraudulent certificates
  http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/
- 2012 - Trustwave issues man-in-the-middle digital certificate
  http://www.computerworld.com/article/2501291/internet/trustwave-admits-issuing-man-in-the-middle-digital-certificate--mozilla-debates-punishment.html
- 2013 - ANSSI issues unauthorized certificates for Google domains
  https://googleonlinesecurity.blogspot.com.au/2013/12/further-improving-digital-certificate.html

SSL/TLS Will Save Us 2015

- Lenovo Is Breaking HTTPS with Superfish
  https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops
- D-Link leaks private keys and passphrases
  https://threatpost.com/d-link-accidentally-leaks-private-code-signing-keys/114727/
- Symantec issuing rogue Google certificates
  https://googleonlinesecurity.blogspot.com/2015/09/improved-digital-certificate-security.html
- Dell ships computers with private keys
  http://krebsonsecurity.com/2015/11/security-bug-in-dell-pcs-shipped-since-815/
- Microsoft leaks private key for Xbox Live
  http://www.pcworld.com/article/3013113/security/microsoft-updates-trust-list-after-private-key-for-xbox-live-leaks.html

DNS Vulnerabilities and Attack Surface



https://conference.apnic.net/data/39/dnssec-final_1425360815.pdf, slide 9

DNSSEC

DNSSEC is a set of extensions(EDNS0) to DNS that guarantees:

- **Origin Authority**
  Data was supplied by a rightful source
- **Data Integrity**
  Data has not been tampered with
- **Authenticated denial of existence**
  Non-existent data can be verified

DNSSEC Resource Records

- **DNSKEY - DNS Key**
  Public keys (ZSK and KSK)
  - **ZSK - Zone Sign Key** signs RRsets in zone
  - **KSK - Key Sign Key** signs the ZSK's DNSKEY
- **RRSIG - Resource Record Signature**
  RRset signature generated from private ZSK
- **DS - Delegation Signer**
  Hash that identifies the KSK's DNSKEY of a delegated zone from the parent zone

Verisign DANE Test Sites

good.dane.verisignlabs.com

There is a valid, signed TLSA record for the certificate of this server.

bad-hash.dane.verisignlabs.com

The TLSA record for this server has an incorrect hash value, although it is correctly signed with DNSSEC.

bad-params.dane.verisignlabs.com

The TLSA record for this server has a correct hash value, incorrect TLSA parameters, and is correctly signed with DNSSEC. NOTE: The current Firefox plugin accepts these TLSA records as valid.

bad-sig.dane.verisignlabs.com

The TLSA record for this server is correct, but the DNSSEC chain-of-trust is broken and/or has a bad signature.

Use DNSSEC on Routers

- **DD-WRT**
  https://www.dd-wrt.com/phpBB2/viewtopic.php?p=966789&highlight=&sid=3d97b7b967f25009ad2eeb7393f2c1e1
- **pfSense / OPNsense**
  https://doc.pfsense.org/index.php/Unbound_DNS_Resolver

These router projects include the Unbound DNS Resolver

Using Validating Resolvers

- **BIND 9** - Response Policy Zones
- **Unbound** - Fast, secure, and
  can temporarily mark zones as insecure
- **Dnsmasq** 2.69 and later - light weight

- **Windows 2008 R2** - yeah

DNSSec is an absolute requirement if we want to … use the Internet for anything non-trivial

Cricket Liu
Leading expert on the Domain Name System (DNS)
“Why you need to deploy DNSSec now,” InfoWorld, Aug 5, 2014

The Internet needs this technology and it needs it now

Vint Cerf
Father of the Internet
"DNSSEC Industry Coalition Meets with Google's Chief Internet Evangelist Vint Cerf and Internet Researcher Dan Kaminsky",
Your Public Interest Registry, March 18 2009

One of the most important security improvements to the Internet ever

Steve Crocker
Internet Pioneer and Chair of the Board of ICANN
“2011 Steve Crocker speaks about DNSSEC Deployment”, Oct 2011

The Truth

Not default for desktops and many appliances

NEED to test! reall dnssec is not enabled(if enabled they are not set to check parent for delegate signature, this means an attacker can disable dnssec. this is done for compatiblity reasons.)

Administrator need to learn to manage

Broken chain of trust, my experiance at CBTL

DNSSEC

DNSSEC ensures credibility of DNS information.

DNSSEC protects against data spoofing and corruption.

DNSSEC adds security, while maintaining backwards compatibility.